EXHIBIT 3

Mesa County Colorado Voting Systems

Report #1 with Forensic Examination and Analysis

September 2021

Mesa County, Colorado, Voting Systems

Report #1 with Forensic Examination and Analysis

15 September 2021

Table of Contents

Executive Summary 1

Introduction 3

Legal References........ 5

Forensic Examination and Analysis Report 7

Forensic Analysis 8

System Identification........ 8

Authenticity and Chain of Custody........ 10

FINDINGS 11

- Overview of System Data Sources 11
- Server Disk Partition Structure Overwritten........ 12
- Website Server Log Files Missing 15
- Server Microsoft SQL Server Installation Log Files Missing 17
- Server Microsoft SQL Server Log Files Missing 19
- EMS Server Dell Server Updates Missing........ 20
- Server 'Administrator' WebCache Log Files Overwritten........ 22
- Server 'emsadmin' WebCache Log Files Overwritten 23
- Server SQL Server Management Studio (SSMS) Log Files Overwritten........ 25
- Server CBS Log Files Overwritten........ 26
- Server Election Databases Missing........ 27
- Server Event Logs Missing/Overwritten 29
- Server System Users are Missing 31
- Server Virtual Directories Log Files Missing........ 32
- Server Windows Defender Log Files Missing/Overwritten........ 33
- Server List of .log files in Before Image that were Deleted. 34
- Significant Number of Logfiles Missing 35
- List of .evtx Event Log Files deleted 36

Analysis Summary 41

Conclusion........ 41

Appendix A. Deleted ".log" files after Dominion Trusted Build update........ 42

Appendix B. Supporting Documentation: File details and hash sets for screenshots 61

Appendix C. Microsoft EVENT log files........ 62

Appendix D. List of Figures........ 76

Appendix E. 2002 Voting Systems Standards (VSS) 77

EXECUTIVE SUMMARY

This report documents initial findings in an ongoing forensic examination of the voting systems of Mesa County, Colorado, used in the November, 2020 General Election. These voting systems represent a portion of overall election systems infrastructure, and this report is limited to the findings of an ongoing investigation. The findings in this report were prepared by the cyber forensic expert retained to advise the County Clerk pursuant to her duties as the county's Chief Election Official as part of the impacted parties' legal team.

Federal law requires the preservation of election records – which includes records in electronic or digital form – for twenty-two months after an election. Colorado law requires the preservation of election records for an additional three months beyond the Federal requirement. The obligation to ensure the integrity of elections and that all election records are preserved pursuant to federal and state law falls to the elected Clerk & Recorder. This report, the first of several, is based on examination of the data obtained from forensic images of the Dominion Voting System EMS server last used in Mesa County for the November, 2020, election, images taken in furtherance of the preservation requirements of federal and state law. Based upon information received by the Clerk's office from various sources in early 2021, the Clerk became concerned that the voting system modifications might jeopardize these preservation and other legal requirements under the responsibility of the County Clerk. For this reason the Clerk ensured a full backup of election records from the County voting systems, both before and after the software modification performed by the vendor and the Secretary of State on May 25-26, 2021, just six months after the November, 2020, election.

Forensic examination[1] found that election records, including data described in the Federal Election Commission's 2002 Voting System Standards (VSS) mandated by Colorado law as certification requirements for Colorado voting systems, have been destroyed on Mesa County's voting system, by the system vendor and the Colorado Secretary of State's office. Because similar system modifications were reportedly performed upon county election servers across the state, it is possible, if not likely, that such data destruction in violation of state and federal law has occurred in numerous other counties.

The extent and manner of destruction of the data comprising these election records is consequential, precluding the possibility of any comprehensive forensic audit of the conduct of any involved election. This documented destruction also undermines the conclusion that these Colorado voting systems and accompanying vendor and Colorado Secretary of State-issued procedures could meet the requirements of Colorado and Federal law, and consequently vitiates the premise of the Colorado Secretary of State certification of these systems for use in Colorado.

Two backup images, using forensic imaging methods, were obtained from the Dominion Voting Systems (DVS) Democracy Suite (D-Suite) Election Management System (EMS) Standard Server in Mesa County, Colorado. The first image was made of that EMS Standard Server in the D-Suite 5.11-CO version configuration, as used in the November, 2020 election. The second image was of the configuration of the EMS Standard Server in the D-Suite 5.13 version configuration, following the modification of the EMS Standard Server by a combined team of DVS vendor personnel and Colorado Secretary of State staff. The forensic information provided in this report is presented using screenshots from forensic analysts' systems running industry-standard forensics software tools. The report includes "before" and "after" screenshots from the forensic tool that shows the differences between the two backup images.

The forensic examination found that numerous logfiles had been deleted or overwritten. These logfiles are required to reconstruct the function of and events taking place on the the voting systems, and based upon information

[1] Many individuals and organizations, some public officials, have made recent claims that no audit performed nor examination conducted on elections or computer-based election systems can be legitimate or credible unless the examiners are "election experts" or accredited election auditors. There is no such thing as an "accredited election auditor," nor are there Federal standards or procedures to credential election auditors.

provided by legal counsel, must, by law, be preserved. By comparing filenames in the two images (before and after the Dominion update on May 25-26, 2021), examination and analysis identified a total of 28,989 files that were deleted. During a software update, some replacement of program files and their related content is normally expected. However the examination found that 695 log and event log files necessary for the determination of election integrity were deleted.

Based upon information provided by legal counsel, Colorado law (Colorado Revised Statute (CRS) § 1-5-601.5) requires that, prior to use in Colorado elections, electronic and computer-based voting systems be certified by the Colorado Secretary of State. This certification is based on the systems' compliance with the requirements of the Federal Electon Commission's 2002 Voting System Standards (VSS), verified by their testing by a Federally-accredited (by vote of the U.S. Election Assistance Commission (EAC)) Voting System Testing Lab (VSTL). While several iterations of newer Voluntary Voting System Guidelines (VVSG) have been issued by the EAC, Colorado's statutory requirement is for compliance with 2002 VSS, which states:

> "Election audit trails provide the supporting documentation for verifying the accuracy of reported election results. They present a concrete, indestructible archival record of all system activity related to the vote tally, and are essential for public confidence in the accuracy of the tally, for recounts, and for evidence in the event of criminal or civil litigation."

The relevant sections of the VSS are cited in Appendix E.

These statutory requirements establish that voting systems are required to generate and preserve, as critical to the ability to determine and reproduce the conditions and details of election conduct using these systems, logfiles of all system functions, including normal activity, connectivity, file and data access, operator- and automated-processes, and errors. Logfiles are critical to the ability to detect improper operation, including the ability to detect malicious intrusions as well as other improper activities and conditions, and configuration changes that could enable alteration of the actual vote count.

Assuming this information to be correct, this forensic examination found that a substantially large number of these requirements have not been met. This examination also found that destruction of critical logfiles has occurred. This destruction is not incidental or minor but is extensive.

The purpose of this initial report is to document these findings and present preliminary evidence demonstrating unacceptable conduct and system defects revealed by the examined images, as necessary for the Chief Election Official to discharge her statutory obligations. The facts and resultant findings support the conclusions that:

1) Election-related data explicitly required to be preserved, as stated in the 2002 VSS criteria referenced in this section, have been destroyed in violation of Federal and State law, and

2) Due to non-compliance with the 2002 VSS requirements, these voting systems and accompanying vendor-provided, Colorado Secretary of state-approved procedures cannot meet the certification requirements of the State of Colorado, and should not have been certified for use in the state.

Comprehensive investigation is required to determine whether these critical failures are the result of malicious intent or negligence, and to what extent the systems may have been compromised or subjected to unauthorized access or operation prior to, during, and after election use. That comprehensive investigation *is beyond the scope of this report*. Subsequent reports will address these issues in detail.

Evidence supporting all of these findings is documented in this report.

Introduction

Election officials, including Secretaries of State, are obligated by law to ensure the integrity of all elections, including the transparency required for citizens to verify that integrity themselves. Modern electronic voting systems are marketed as an efficient solution to streamline the voting process and allow for automated collection, tabulation, and reporting of election results, but the efficiency they promise comes at a cost.

The necessary measures and safeguards to ensure the integrity of the systems and their operation against a severe, mounting and ever-evolving threat from sophisticated nation-state and non-nation-state actors are so complex and dynamic as to outpace the limited capabilities and resources of our government, at all levels. While minimal security safeguards may be within government capacity, modern computer-based voting systems are extremely complex and difficult to secure, even for cybersecurity experts, and since voting systems are not under the direct control of the Federal government's top security experts, any government assurances about the sufficiency of those safeguards can serve only to mislead citizens and policy-makers. Even critical defense systems, relentlessly monitored and defended by highly-trained teams using costly, sophisticated tools, are at risk and are frequently compromised, sometimes before procurement. Earlier generations of voting systems relied on simple, human-scale safeguards, for example "air gaps"– that is – to have no wired network connection to the system. But miniaturized wireless communication technologies and networks have proliferated, with billions of wireless devices installed or in use, and malicious actors have developed sophisticated attacks to bypass air gaps, compromise every kind of hardware, firmware, and software, often before they even come into customer or user possession, and to move laterally through networked systems, often undetected. Supply-chains for these systems, from the initiation of the design of integrated circuits and electronic components, most manufactured overseas with little U.S. insight or oversight, through the fabrication, testing, assembly, integration, and operation of these complex composite systems, are vulnerable and untrustworthy for critical functions of government and lucrative economic and national security targets. For all these reasons logfiles, such as those that have been deleted by the Dominion "Trusted Build" update must be preserved to document the complete operation of the computer system and voting applications, and to be able to verify the authenticity, integrity and accuracy of the vote.

The feature size of individual circuits in the chipsets and components of our voting system computers is at the nanoscale, smaller than the smallest known virus particle, and less than 3/10,000ths of the width of a human hair. So we have lost the ability, if we ever had it, to visually verify what is really happening, even at the physical level, in our computer-based voting system. Regardless of how the systems appear to be configured to authorized users and poll-watchers, the functionality and connectivity in these computers can be enabled and modified remotely and wirelessly, or by the introduction of embedded codes on scanned paper, or triggered by specific unforeseeable and indiscernible predetermined software and hardware conditions, or by specific timing events, or by geographic location, or by the proximity of other devices or combinations of any of these means.

For example, some Colorado voting systems ordered as specified by the voting system vendors, from foreign manufacturing and assembly facilities, have included "Integrated Dell Remote Access Controllers (IDRAC)," which are designed to allow "out-of-band" remote management of those systems, meaning that the computers are explicitly equipped to be controlled by remote automated programs or by individuals other than those logged in locally. Through the IDRAC, voting systems might have any aspect of their Basic Input/Output System (BIOS), operating system, or applications controlled or modified, including the addition and deletion of user accounts, the enabling of communications components like wireless networking cards, and the modification, installation, removal or configuration of software and settings. Like the inclusion of multi-band wireless networking cards, similarly specified and ordered for Colorado voting systems by the vendor, there is no excuse or rational justification for the inclusion of components like these, and the fact that the entirety of U.S. voting system regulatory processes and institutions can apparently neither detect, note, nor address these gross vulnerabilities eviscerates the notion that our computer-based voting systems have been secured.

Faced with incredible miniaturization, the importance of logfiles which are records of operation of a computer system, are more important than ever in managing this technology. When the computer is part of a national critical infrastructure, these operational records become essential, not only for troubleshooting or security alone, but for the integrity of the system itself as a component of the National Critical Infrastructure.

For the purposes of this document and ensuing discussion, two terms are defined to differentiate and clarify the evidentiary findings. *Election Data* is all information regarding Ballot Design, Ballot Marking, Electronic scanning of completed ballots, interpretation of the intention of each voter's choice, including human, machine generated or programatic adjudication in the event that the election system is unable to determine conclusively the correct vote input from any specific ballot, tabulation of the actual vote including the databases used to actually contain the raw vote totals, scanned ballot images and Voter Registration and Voter identification information associated with any specific election, as well as the actual vote totals. This includes a complete record of any realtime changes in databases resident in the cloud such as voter registration data. *Election-Related Data* includes all of the computer log and configuration data that document the complete configuration state and operation of the entire computer system and infrastructure upon which Election Software is executed, as well as the operating system of devices that store log and election data such as Network Attached Storage (NAS). Also included in Election-Related data are logs and configuration of network Routers, Firewalls, Intrusion Detection Systems, Intrusion Prevention Systems, and other network security devices, including VPNs and more[2].

Both Election Data AND Election-Related Data must be preserved as "Election Records" under the law, and this is broadly addressed in both the 2002 VSS and the EAC's successor versions of VVSG.

Securing computer systems is a non-trivial task. It involves a litany of processes, including, but not limited to:

- Engineering systems with a focus on security
- Building systems to meet published high-security standards and applicable regulations
- Patching systems to ensure that vulnerabilities are removed
- Securing networks to ensure highly controlled access
- Logging of all communications, processes, access, system modifications
- Auditing of systems and logs regularly to ensure ongoing compliance
- Adequate training and certification for engineers, administrators, and system users
- Adherence to Industry Best Practices, for example, emphasis on password strength and configured security and group policies

These, among other measures, will help to ensure what is known as the CIA triad. The CIA triad represents the three pillars of information security: confidentiality, integrity, and availability, as follows:

[2] Log and configuration examination of not only the computer system(s) but also all network systems are critical to forensic examination. Compromise of any unrelated information (e.g. plain-text cofiguration data containing normally-encrypted passwords) can be easily prevented, so long as simple, quick forensic examiner and cyber professional industry standards are used to obfuscate private and sensitive data from the network device files.

Confidentiality – preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Integrity — guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity

Availability – ensuring timely and reliable access to and use of information

Integrity
Data

Failure in any of the three pillars can and generally will result in a compromise of the system. Failure in the integrity component can have dire consequences for public perception, election results, the future of our government and our country.

Industry-standard forensics analysis tools were applied to the forensic examination.

Information was forensically evaluated using backup images taken from a Mesa County Election server configured for DVS D-Suite 5.11-CO on Sunday, May 23, 2021, before its modification by Dominion Voting Systems and the Colorado Secretary of State to DVS D-Suite 5.13, and again on Wednesday, May 26, 2021, after the update had been applied. This server was the primary system that was used to process election data in Mesa County for the 2020 general election.The EMS server configuration and administrative standards were prepared by Dominion Voting Systems (DVS), running a combination of COTS and proprietary DVS software, and certified for use by the Colorado Secretary of State. Our conclusions include determining that this system not only failed to meet any reasonable standard or statutory requirement for cybersecurity but was also subject to removal of critical information (data destruction).

Our findings include serious irregularities that resulted in the loss of data integrity on the server, including election data and election-related data.

LEGAL REFERENCES

Several Federal and Colorado state legal standards apply to the preservation and definition of election records, applicable to the data generated by and resident on voting systems. Beginning with 52 USC §20701, retention and preservation of records and papers by officers of elections; deposit with custodian; penalty for violation, which states:

> Every officer of election shall retain and preserve, for a period of twenty-two months from the date of any general, special, or primary election of which candidates for the office of President, Vice President, presidential elector, Member of the Senate, Member of the House of Representatives, or Resident Commissioner from the Commonwealth of Puerto Rico are voted for, all records and papers which come into his possession relating to any application, registration, payment of poll tax, or other act requisite to voting in such election, except that, when required by law, such records and papers may be delivered to another officer of election and except that, if a State or the Commonwealth of Puerto Rico designates a custodian to retain and preserve these records and papers at a specified place, then such records and papers may be deposited with such custodian, and the duty to retain and preserve any record or paper so deposited shall devolve upon such custodian. Any officer of election or custodian who willfully fails to comply with this section shall be fined not more than $1,000 or imprisoned not more than one year, or both.

In addition to 52 USC §20701, multiple sections of Colorado Revised Statutes (CRS) appear applicable, including:

> CRS 1-5-601.5. Compliance with federal requirements (Effective until July 1, 2022)
>
> All voting systems and voting equipment offered for sale on or after May 28, 2004, shall meet the voting systems standards that were promulgated in 2002 by the federal election commission. At his or her discretion, the secretary of state may require by rule that voting systems and voting equipment satisfy voting systems standards promulgated after January 1, 2008, by the federal election assistance commission as long

> as such standards meet or exceed those promulgated in 2002 by the federal election commission. Subject to section 1-5-608.2, nothing in this section shall be construed to require any political subdivision to replace a voting system that is in use prior to May 28, 2004.
>
> CRS 1-7-802. Preservation of election records
>
> The designated election official shall be responsible for the preservation of any election records for a period of at least twenty-five months after the election or until time has expired for which the record would be needed in any contest proceedings, whichever is later. Unused ballots may be destroyed after the time for a challenge to the election has passed. If a federal candidate was on the ballot, the voted ballots and any other required election materials shall be kept for at least twenty-five months after the election.
>
> 1-13-716. Destroying, removing, or delaying delivery of election records
>
> (1) No person shall willfully destroy, deface, or alter any ballot or any election records or willfully delay the delivery of any such ballots or election records, or take, carry away, conceal, or remove any ballot, ballot box, or election records from the polling location or drop-off location or from the possession of a person authorized by law to have the custody thereof, or aid, counsel, procure, advise, or assist any person to do any of the aforesaid acts.
>
> (2) No election official who has undertaken to deliver the official ballots and election records to the county clerk and recorder shall neglect or refuse to do so within the time prescribed by law or shall fail to account fully for all official ballots and other records in his charge. Informality in the delivery of the ballots and election records shall not invalidate the vote of any precinct if such records are delivered prior to the canvassing of the votes by the county board of canvassers.
>
> (3) Any person who violates any provision of this section is guilty of a misdemeanor and, upon conviction thereof, shall be punished as provided in section 1-13-111.

And several sections of the Code of Colorado Regulations appear applicable, including:

> 8 CCR 1505-1, Rule 21, 21.4.2: All voting systems must meet the requirements of the 2002 Voting Systems Standards, parts 5 – 7 of article 5 of title 1, CRS, as amended, and this Rule 21.

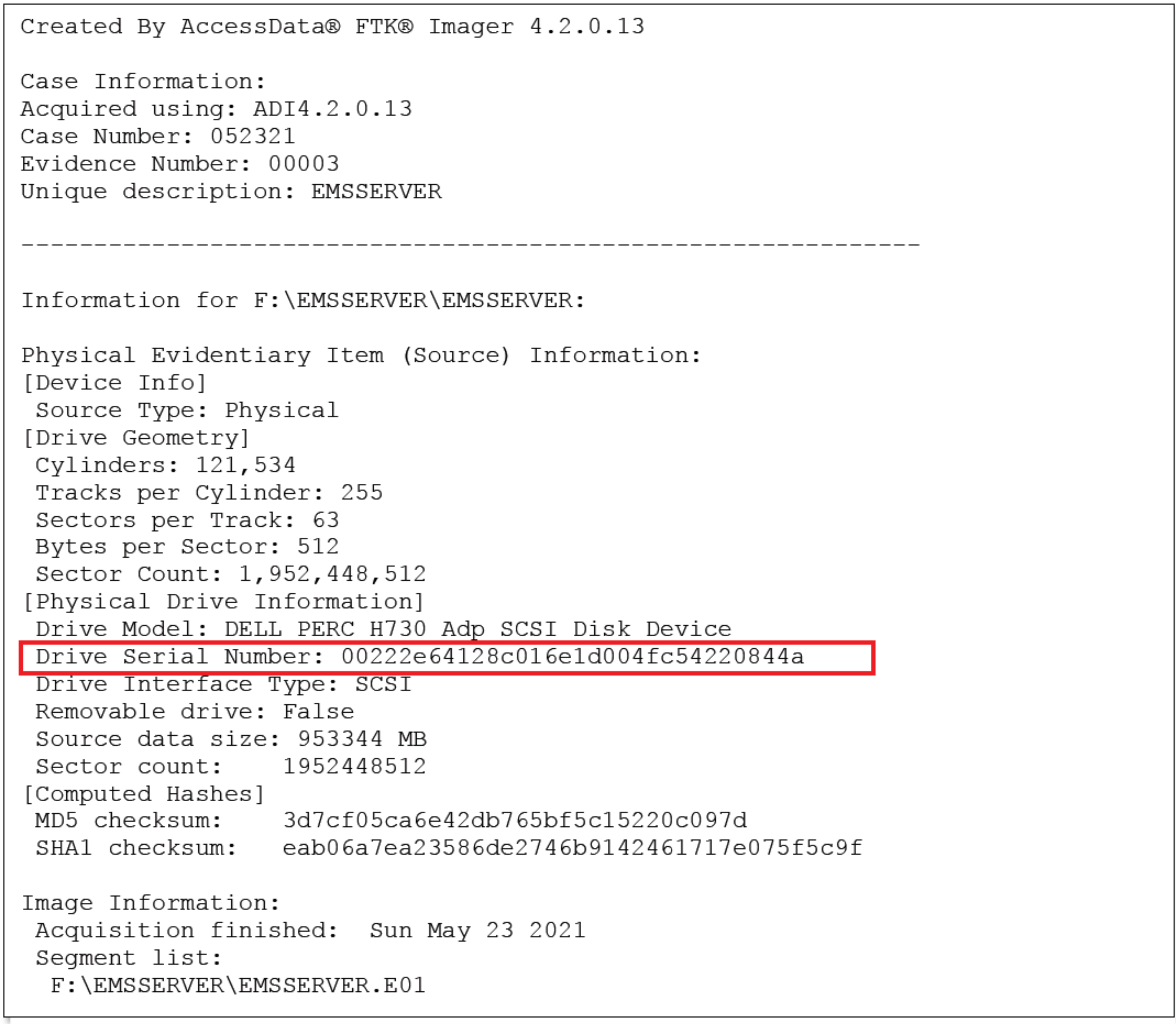
FORENSIC EXAMINATION AND ANALYSIS REPORT

SYSTEM IDENTIFICATION

The server that was analyzed is capable of operating on a small local area network (LAN). The network consists of several systems, including servers and workstations running in a non-virtualized environment. The server that we evaluated was named EMSSERVER. It is running the Microsoft Windows Server 2016 Standard operating system.

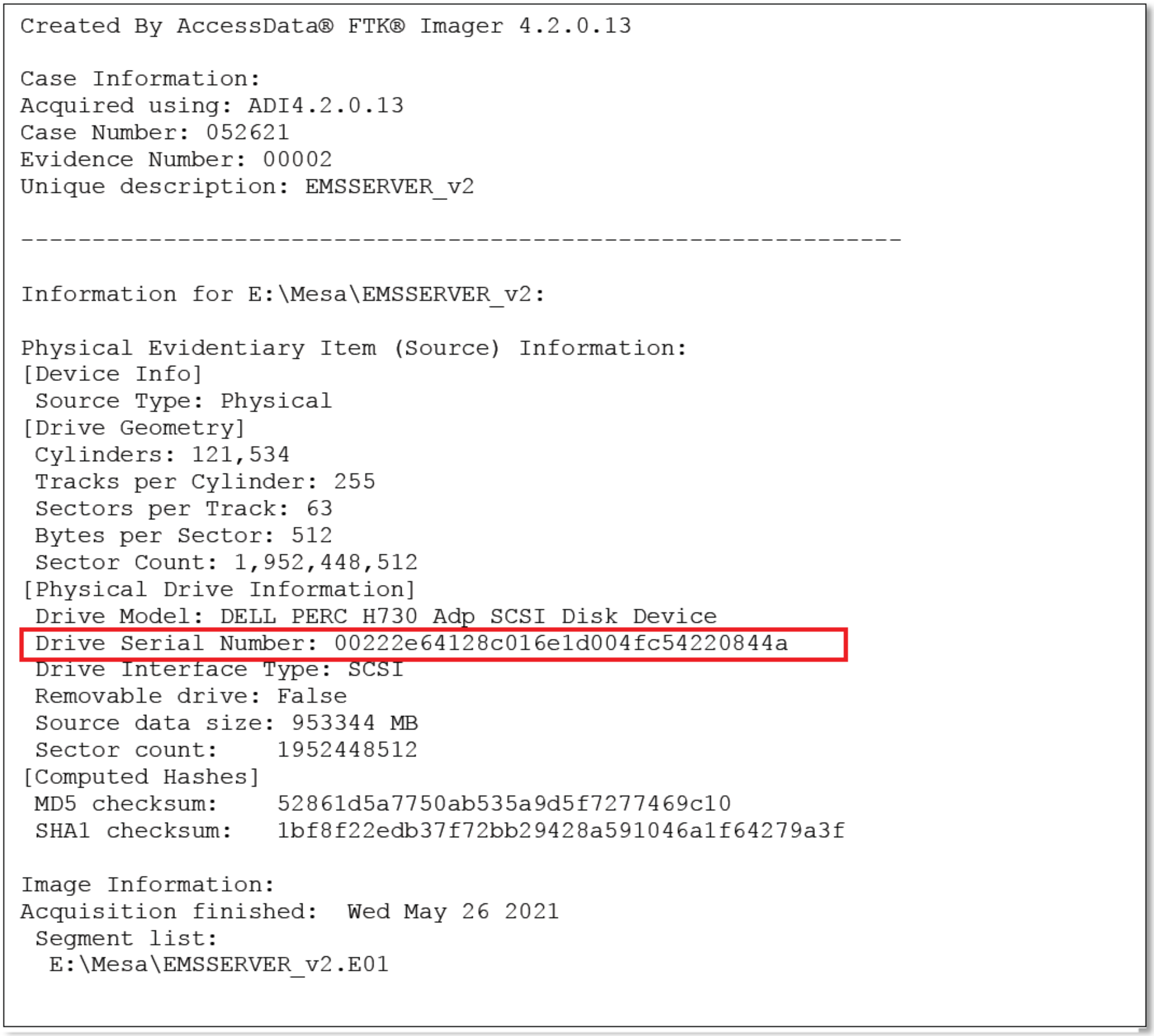
The forensic evaluation and reviews were based upon a forensic image archive collected from the Mesa County Dominion EMS Server. The Before and After forensic images were collected from the same server and same hard drive, as documented below, from the actual acquisition. The serial number of the hard drive shown in each collection data set verifies the data origin to be the same physical device.

Figure 1 – EMS Server (5.11-CO) Image Attributes Before



```
Created By AccessData® FTK® Imager 4.2.0.13

Case Information:
Acquired using: ADI4.2.0.13
Case Number: 052321
Evidence Number: 00003
Unique description: EMSSERVER

--------------------------------------------------------------


Information for F:\EMSSERVER\EMSSERVER:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 121,534
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 1,952,448,512
[Physical Drive Information]
 Drive Model: DELL PERC H730 Adp SCSI Disk Device
 Drive Serial Number: 00222e64128c016e1d004fc54220844a
 Drive Interface Type: SCSI
 Removable drive: False
 Source data size: 953344 MB
 Sector count:    1952448512
[Computed Hashes]
 MD5 checksum:    3d7cf05ca6e42db765bf5c15220c097d
 SHA1 checksum:   eab06a7ea23586de2746b9142461717e075f5c9f

Image Information:
 Acquisition finished:  Sun May 23 2021
 Segment list:
  F:\EMSSERVER\EMSSERVER.E01
```

Figure 2 - EMS Server (5.13) Image Attributes After



```
Created By AccessData® FTK® Imager 4.2.0.13

Case Information:
Acquired using: ADI4.2.0.13
Case Number: 052621
Evidence Number: 00002
Unique description: EMSSERVER_v2

--------------------------------------------------------------

Information for E:\Mesa\EMSSERVER_v2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 121,534
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 1,952,448,512
[Physical Drive Information]
 Drive Model: DELL PERC H730 Adp SCSI Disk Device
 Drive Serial Number: 00222e64128c016e1d004fc54220844a
 Drive Interface Type: SCSI
 Removable drive: False
 Source data size: 953344 MB
 Sector count:    1952448512
[Computed Hashes]
 MD5 checksum:    52861d5a7750ab535a9d5f7277469c10
 SHA1 checksum:   1bf8f22edb37f72bb29428a591046a1f64279a3f

Image Information:
Acquisition finished:  Wed May 26 2021
 Segment list:
  E:\Mesa\EMSSERVER_v2.E01
```

Two backup images were obtained, using forensic imaging methods, from the Dominion Voting Systems (DVS) Democracy Suite (D-Suite) Election Management System (EMS) Standard Server in Mesa County, Colorado. The first image was made of that EMS Standard Server in the D-Suite 5.11-CO version configuration, as used in the November, 2020 election on May 23, 2021. The second image was of the configuration of the EMS Standard Server in the D-Suite 5.13 version configuration, following the modification of the EMS Standard Server by a combined team of Dominion Voting System vendor personnel and Colorado Secretary of State (SecState) staff, on May 26, 2021. A forensic image (forensic copy) is a bit-by-bit, sector-by-sector duplicate of a physical storage device using specialized hardware and software; it is a much more comprehensive representation of the state and configuration of the imaged system than could be obtained using simple file backup methods. The images include all files, folders, and unallocated, free, and slack space. These forensic images include not only all the files visible to the server operating system but also deleted files and fragments of files left in the slack and free space but every digital bit of data present on the storage medium, in this case, a SCSI hard disk. When forensic images are acquired, a hash function, also known as a Message Digest, is computed. This hash can be used at any time to validate the integrity of the image to ensure that it has not been edited, modified, or changed in any way. The hash function result from the acquisition of data appears in the text above but also appears inside each respective archive and authenticates the data by demonstrating that it has not changed since it was acquired.

These two images were evaluated to gather technical information, including the integrity of the data stored on the system. No effort was made to reverse-design, de-compile or reverse-engineer the Dominion software. Configuration, which is relevant to the operation of the system, was examined to determine whether improper settings could allow undesirable results and were found to contain such errors. Results relevant to this investigation are documented below. Additional supporting documentation can be found in the appendixes. They include directory listings for many of the directories seen in the screenshots and contain complete filenames, full path names where the files are located, and file hashes.

We have included screenshots that can be used to review and verify these findings. These screenshots were obtained from the forensic images of the Dominion server.

AUTHENTICITY AND CHAIN OF CUSTODY

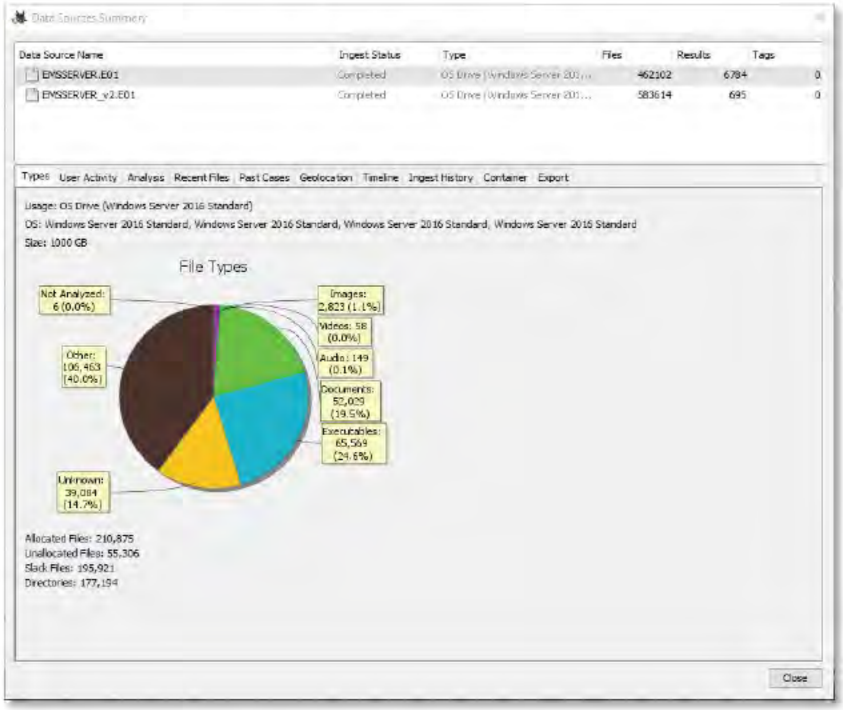
Digital chain of custody is the record of preservation of digital evidence from collection to presentation in the court of law. This is an essential part of the digital investigation process. The chain of custody is probative that the digital evidence presented to the court remains as originally collected, without tampering. The two images analyzed in this report were obtained through AccessData FTK Imager 4.2.0.13. The serial number on the EMS Server drive on both images match, thus establishing that both images were taken from the same physical drive. I have reviewed the documented chain of custody for both images and have determined that the chain of custody is complete from the forensic operator utilizing FTK Imager through the source from which I directly received these images. (Because of the pending civil litigation and criminal investigation, the written documentation remains in the custody of counsel for later introduction in court proceedings and thus cannot be released as part of this report.) Further confirmation that these are genuine images from the Mesa County EMS Server has been provided by the Colorado Secretary of State's office. See:

https://www.sos.state.co.us/pubs/newsRoom/pressReleases/2021/PR20210817MesaCounty.html

FINDINGS

Overview of System Data Sources

Figure 3 – EMS Server (5.11-CO) System Data Sources Before

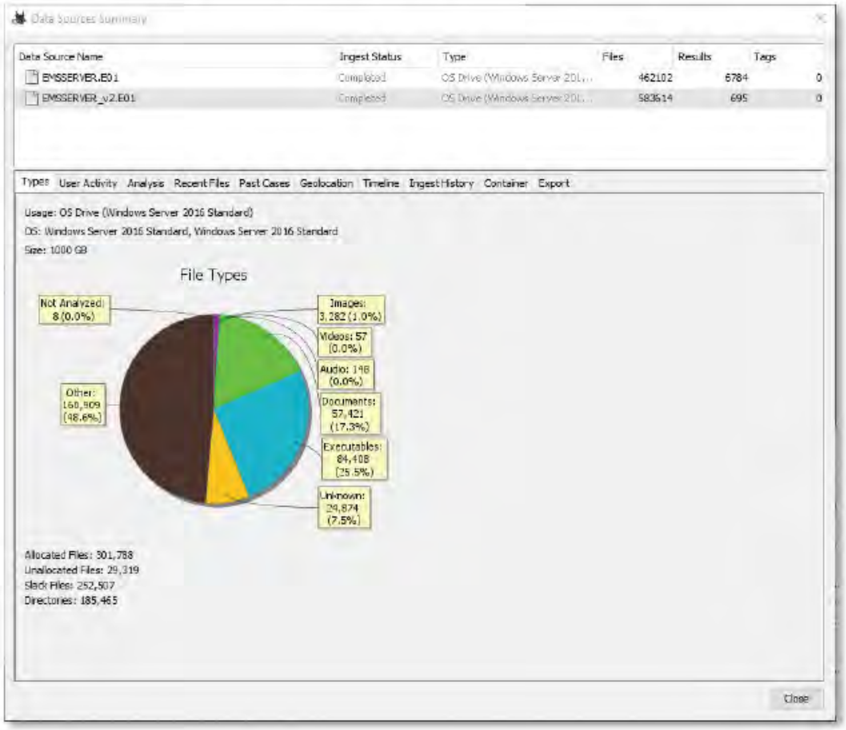


Data Source Name	Ingest Status	Type	Files	Results	Tags
EMSSERVER.E01	Completed	OS Drive (Windows Server 201…	462102	6784	0
EMSSERVER_v2.E01	Completed	OS Drive (Windows Server 201…	583614	695	0

Usage: OS Drive (Windows Server 2016 Standard)
OS: Windows Server 2016 Standard, Windows Server 2016 Standard, Windows Server 2016 Standard, Windows Server 2016 Standard
Size: 1000 GB

Allocated Files: 210,875
Unallocated Files: 55,306
Slack Files: 195,921
Directories: 177,194

Figure 4 - EMS Server (5.13) System Data Sources After



Data Source Name	Ingest Status	Type	Files	Results	Tags
EMSSERVER.E01	Completed	OS Drive (Windows Server 201…	462102	6784	0
EMSSERVER_v2.E01	Completed	OS Drive (Windows Server 201…	583614	695	0

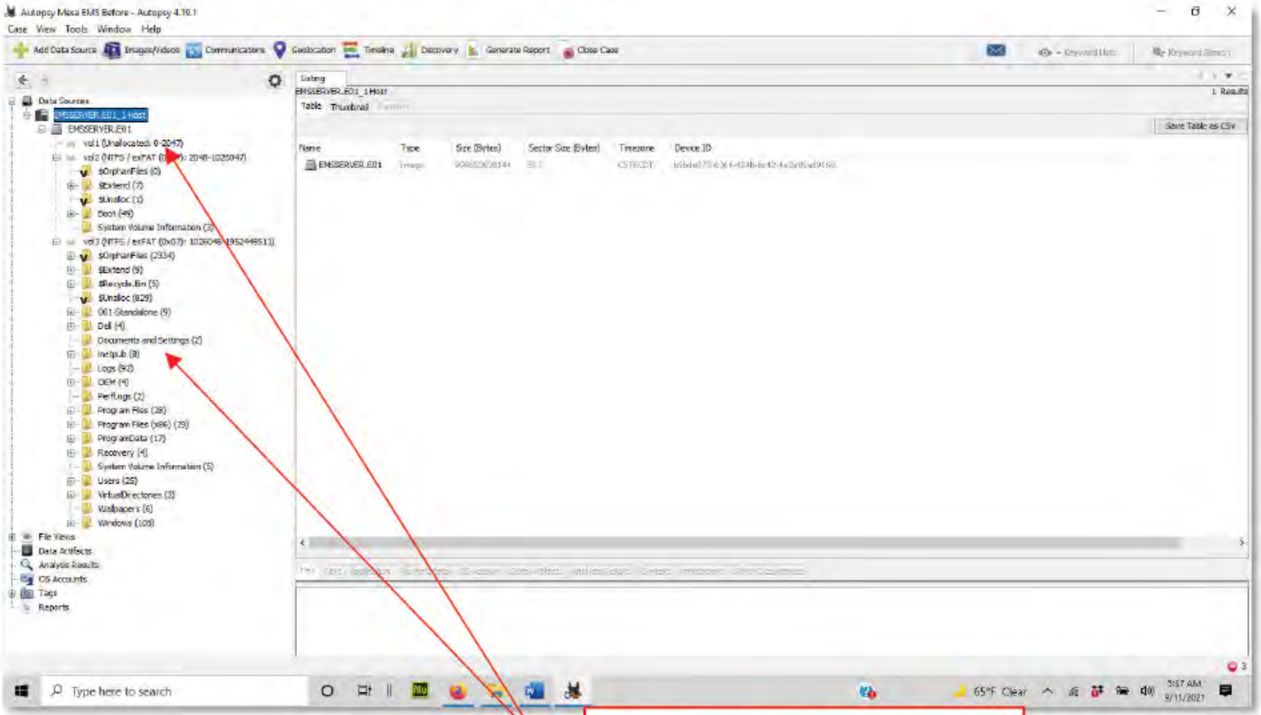
Usage: OS Drive (Windows Server 2016 Standard)
OS: Windows Server 2016 Standard, Windows Server 2016 Standard
Size: 1000 GB

Allocated Files: 301,788
Unallocated Files: 29,319
Slack Files: 252,507
Directories: 185,465

Server Disk Partition Structure Overwritten

Purpose: *The disk partition structure is the structure of how the hard drive is divided up.*

Figure 5 - EMSSERVER (5.11-CO) Disk Partition Structure Before



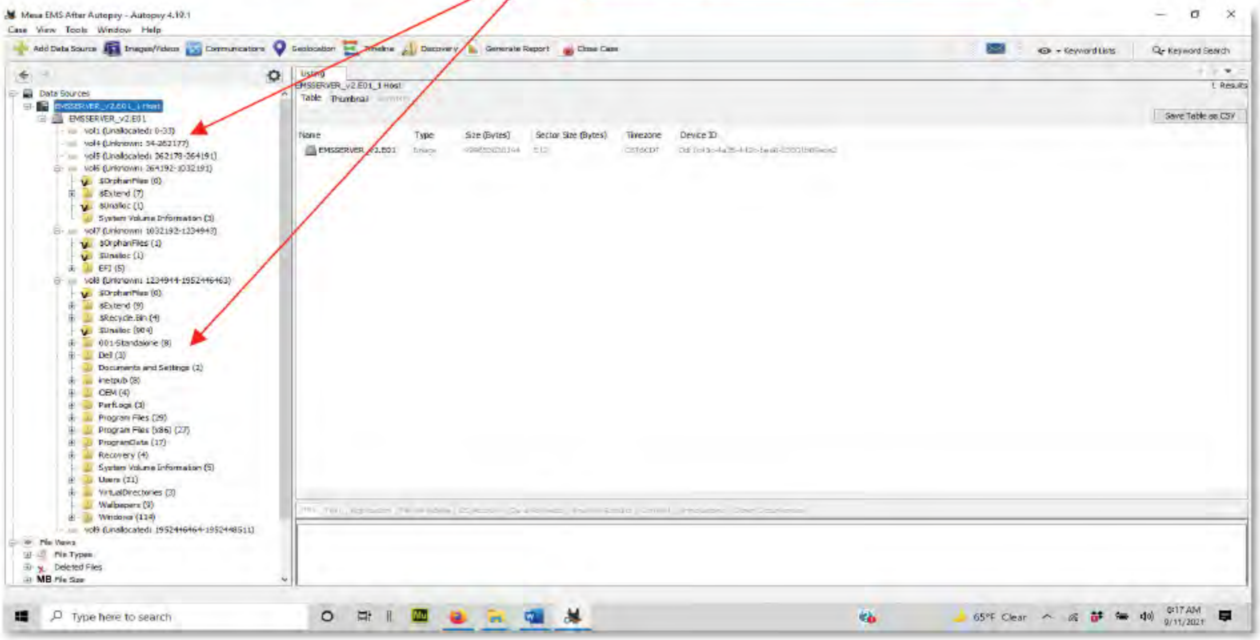
```
Data Sources
  EMSSERVER.E01_1 Host
    EMSSERVER.E01
      vol1 (Unallocated: 0-2047)
      vol2 (NTFS / exFAT (0x07): 2048-1026047)
        $OrphanFiles (0)
        $Extend (7)
        $Unalloc (1)
        Boot (49)
        System Volume Information (3)
      vol3 (NTFS / exFAT (0x07): 1026048-1952448511)
        $OrphanFiles (2334)
        $Extend (9)
        $Recycle.Bin (5)
        $Unalloc (829)
        001-Standalone (9)
        Dell (4)
        Documents and Settings (2)
        inetpub (8)
        Logs (92)
        OEM (4)
        PerfLogs (2)
        Program Files (28)
        Program Files (x86) (29)
        ProgramData (17)
        Recovery (4)
        System Volume Information (5)
        Users (25)
        VirtualDirectories (3)
        Wallpapers (6)
        Windows (108)
```

EMSSERVER.E01_1 Host

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
EMSSERVER.E01	Image	999653638144	512	CST6CDT	b5bda073-6364-424b-bc42-4e2a05ad9168

Note Changes in Disk Volumes and Directory Structures

Figure 6- EMSSERVER (5.13) Disk Partition Structure After

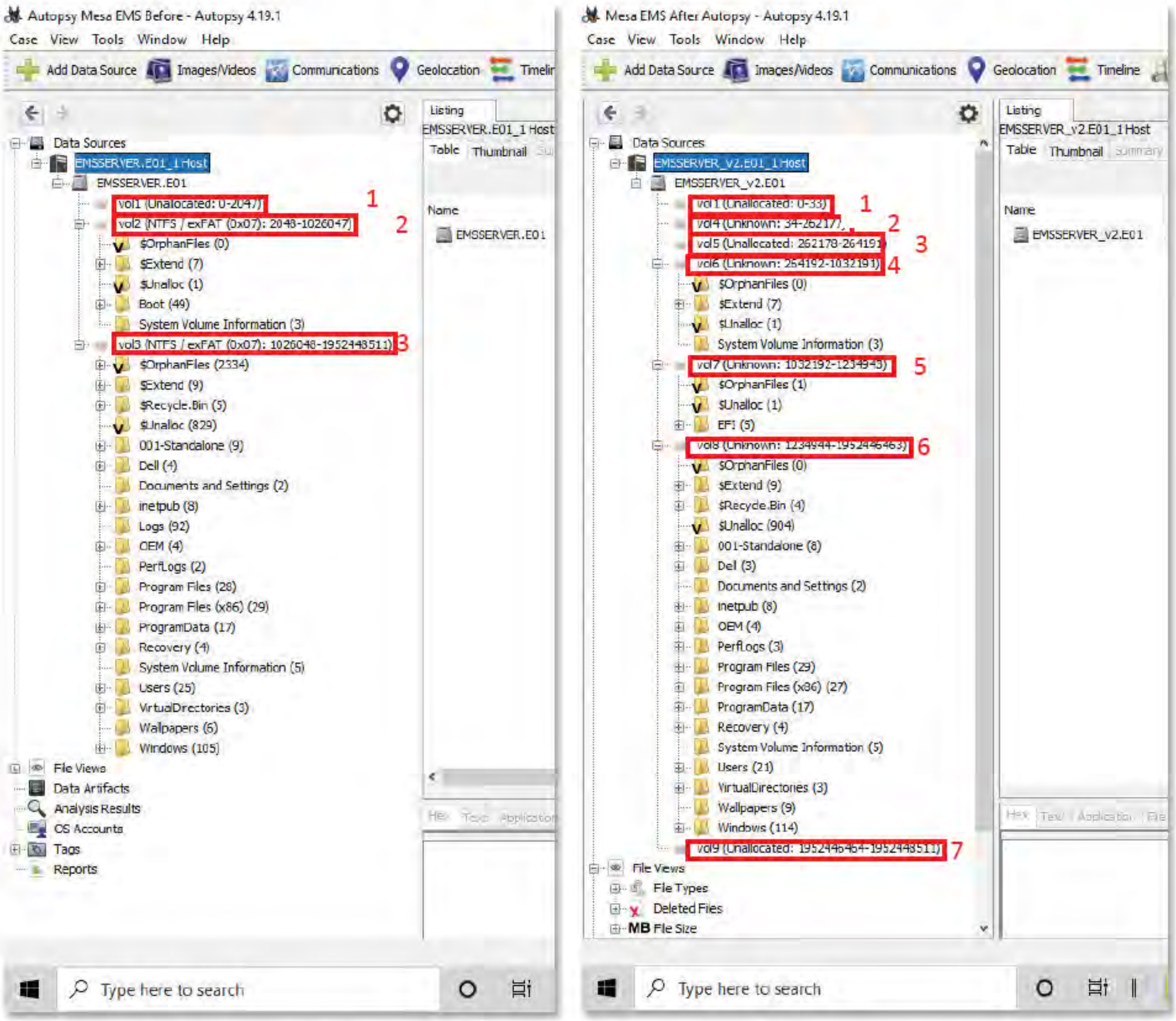


```
Data Sources
  EMSSERVER_v2.E01_1 Host
    EMSSERVER_v2.E01
      vol1 (Unallocated: 0-33)
      vol4 (Unknown: 34-262177)
      vol5 (Unallocated: 262178-264191)
      vol6 (Unknown: 264192-1032191)
        $OrphanFiles (0)
        $Extend (7)
        $Unalloc (1)
        System Volume Information (3)
      vol7 (Unknown: 1032192-1234943)
        $OrphanFiles (1)
        $Unalloc (1)
        EFI (5)
      vol8 (Unknown: 1234944-1952446463)
        $OrphanFiles (0)
        $Extend (9)
        $Recycle.Bin (4)
        $Unalloc (904)
        001-Standalone (8)
        Dell (3)
        Documents and Settings (2)
        inetpub (8)
        OEM (4)
        PerfLogs (3)
        Program Files (29)
        Program Files (x86) (27)
        ProgramData (17)
        Recovery (4)
        System Volume Information (5)
        Users (21)
        VirtualDirectories (3)
        Wallpapers (9)
        Windows (114)
      vol9 (Unallocated: 1952446464-1952448511)
```

EMSSERVER_v2.E01_1 Host

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
EMSSERVER_v2.E01	Image	999653638144	512	CST6CDT	[illegible]

Figure 7 - Server Disk Partition and Directory Changes



Before Dominion Update

After Dominion Update

Computer hard disk drives are data storage devices that must be prepared before use – specifically, they must be partitioned into logical disk volumes and then formatted. Partitioning a hard disk drive is the equivalent of scoring horizontal and vertical rule lines onto blank paper, and then numbering each line, preparing that paper for the orderly recording and look-up of information. A disk is partitioned to organize information into sets of related data. A partition creates a logical drive, C:, D:, E:, etc., that the Master Boot Record (MBR) or Globally Unique Identifier (GUID) Partition Table, which are like maps of the partitioned and formatted memory storage locations on the hard drive, can then use to write and read stored data.

Creation of such a partition, if previous partitions are not preserved, destroys the "map" of underlying data and data locations when the partition is formatted. The previous partition data is then only recoverable by forensic techniques, and is vulnerable to complete destruction if overwritten by data stored according to the new partition "map." Note that in the before image above, each disk partition (Labeled "volX," e.g. "vol1," for "volume") is identified together with the addresses of the beginning block and ending block for each volume.

By comparing the images, it is evident that the disk was re-partitioned, reformatted, and the previous data map completely destroyed by overwriting it with new data, rendering the prior data (mostly) unrecoverable.

Forensic examination of the system can reveal remnants of deleted data. When a computer deletes a file, it does not erase the data; it merely changes the first character of the filename to a non-printable character recognized by software that accesses the disk. This first character tells the operating system to no longer display the file as it is marked as a deleted file, and the space occupied by the disk is marked as reusable.

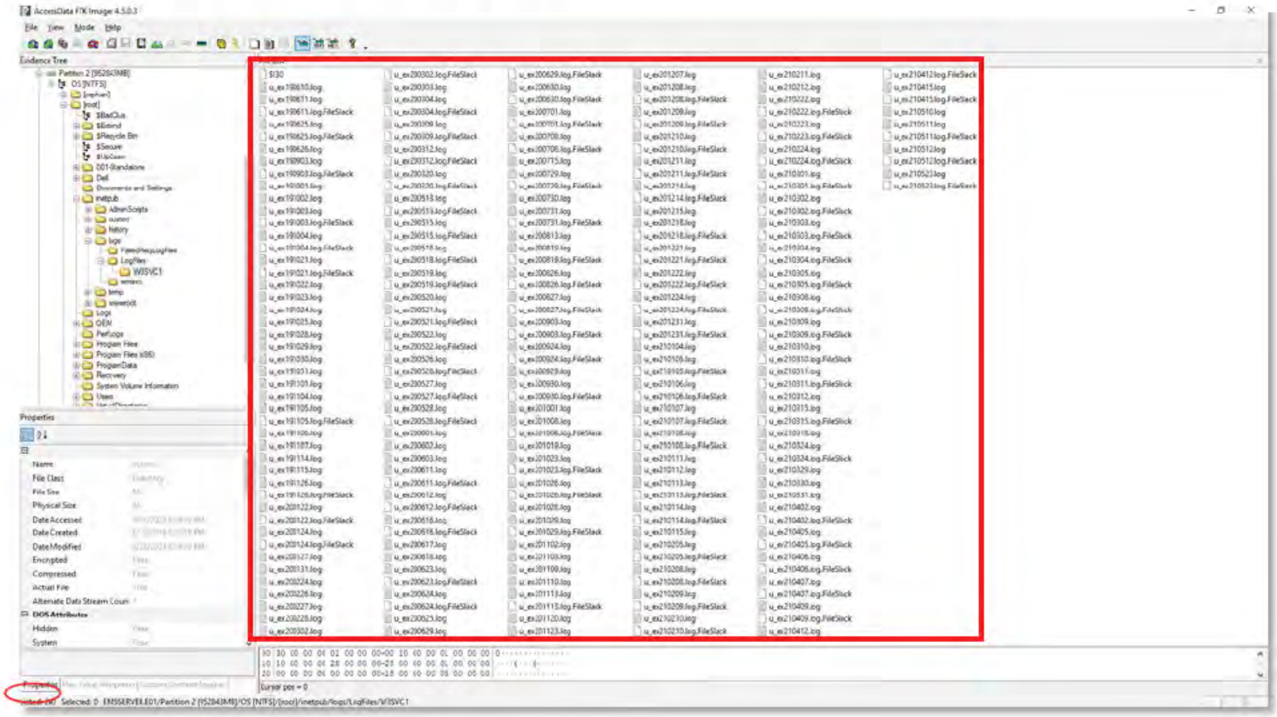
Each block on the disk is the smallest unit of disk space that can be used. The size of all blocks on the disk are determined when the disk is formatted. The smallest disk block size in common use is 512 bytes. Even if a file only occupies 50 bytes of disk space, the entire 512 byte block is marked as "in use".

If a file of 500 bytes is written to the disk, it occupies one block of disk space, with the last 12 bytes (on a newly formatted disk) each containing the numeric value zero (0). If this file is then deleted, and a file of 50 bytes is written to the same disk block, the first 50 bytes of the block contain the new file, and the next remaining 450 bytes of the disk block contain the data from the deleted file that previously occupied the disk block (followed by the 12 null (0) bytes of data). This data remnant is referred to as "File Slack Space" and is defined as any previous remnant data that remains on the disk and is not accessible via the operating system nor allocated as an accessible file.

Special forensic software is required to access file slack space, and the data it contains are partial remnants of previous system data. This data may be of use in forensic investigation, and forensic tools often identify it. File Slack is identified here for clarity and better understanding of these data.

Website Server Log Files Missing

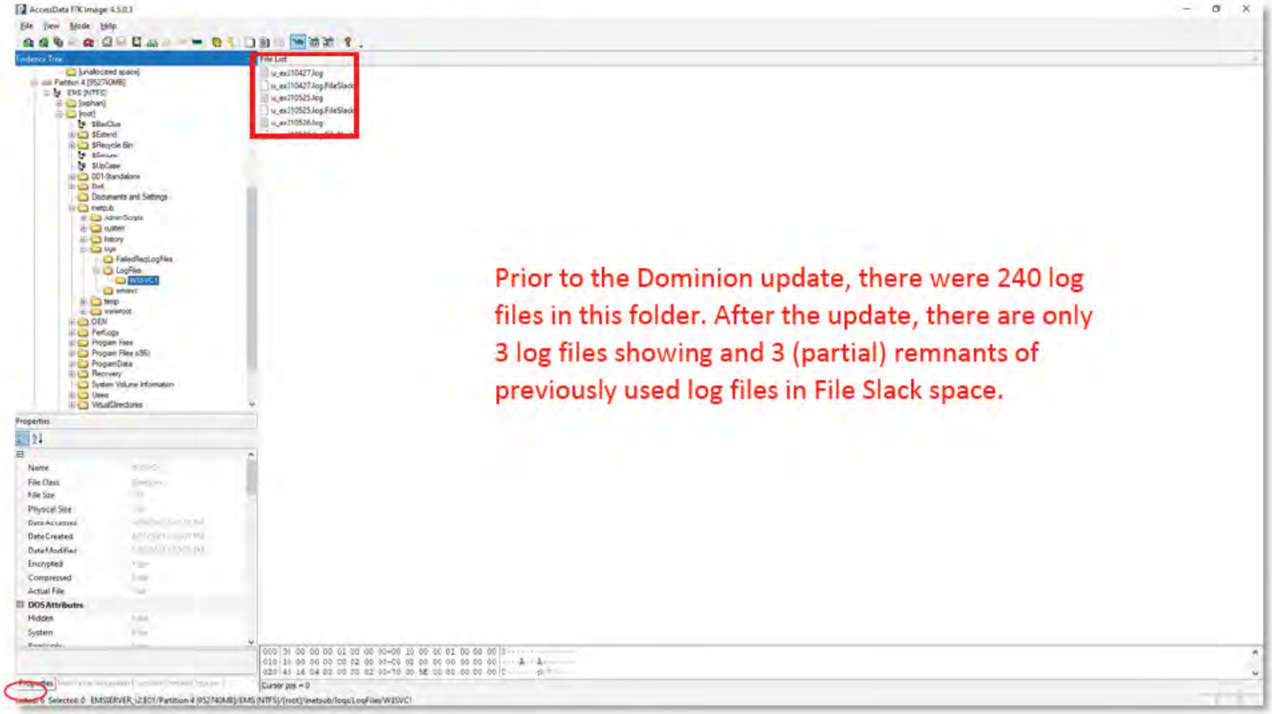
Figure 8 - EMS Server (5.11-CO) Web Server Log Files Before



```
$I30                          u_ex200302.log.FileSlack   u_ex200629.log.FileSlack   u_ex201207.log             u_ex210211.log             u_ex210412.log.FileSlack
u_ex190610.log                u_ex200303.log             u_ex200630.log             u_ex201208.log             u_ex210212.log             u_ex210415.log
u_ex190611.log                u_ex200304.log             u_ex200630.log.FileSlack   u_ex201208.log.FileSlack   u_ex210222.log             u_ex210415.log.FileSlack
u_ex190611.log.FileSlack      u_ex200304.log.FileSlack   u_ex200701.log             u_ex201209.log             u_ex210222.log.FileSlack   u_ex210510.log
u_ex190625.log                u_ex200309.log             u_ex200701.log.FileSlack   u_ex201209.log.FileSlack   u_ex210223.log             u_ex210511.log
u_ex190625.log.FileSlack      u_ex200309.log.FileSlack   u_ex200708.log             u_ex201210.log             u_ex210223.log.FileSlack   u_ex210511.log.FileSlack
u_ex190626.log                u_ex200312.log             u_ex200708.log.FileSlack   u_ex201210.log.FileSlack   u_ex210224.log             u_ex210512.log
u_ex190903.log                u_ex200312.log.FileSlack   u_ex200715.log             u_ex201211.log             u_ex210224.log.FileSlack   u_ex210512.log.FileSlack
u_ex190903.log.FileSlack      u_ex200320.log             u_ex200729.log             u_ex201211.log.FileSlack   u_ex210301.log             u_ex210523.log
u_ex191001.log                u_ex200320.log.FileSlack   u_ex200729.log.FileSlack   u_ex201214.log             u_ex210301.log.FileSlack   u_ex210523.log.FileSlack
u_ex191002.log                u_ex200513.log             u_ex200730.log             u_ex201214.log.FileSlack   u_ex210302.log
u_ex191003.log                u_ex200513.log.FileSlack   u_ex200731.log             u_ex201215.log             u_ex210302.log.FileSlack
u_ex191003.log.FileSlack      u_ex200515.log             u_ex200731.log.FileSlack   u_ex201218.log             u_ex210303.log
u_ex191004.log                u_ex200515.log.FileSlack   u_ex200813.log             u_ex201218.log.FileSlack   u_ex210303.log.FileSlack
u_ex191004.log.FileSlack      u_ex200518.log             u_ex200819.log             u_ex201221.log             u_ex210304.log
u_ex191021.log                u_ex200518.log.FileSlack   u_ex200819.log.FileSlack   u_ex201221.log.FileSlack   u_ex210304.log.FileSlack
u_ex191021.log.FileSlack      u_ex200519.log             u_ex200826.log             u_ex201222.log             u_ex210305.log
u_ex191022.log                u_ex200519.log.FileSlack   u_ex200826.log.FileSlack   u_ex201222.log.FileSlack   u_ex210305.log.FileSlack
u_ex191023.log                u_ex200520.log             u_ex200827.log             u_ex201224.log             u_ex210308.log
u_ex191024.log                u_ex200521.log             u_ex200827.log.FileSlack   u_ex201224.log.FileSlack   u_ex210308.log.FileSlack
u_ex191025.log                u_ex200521.log.FileSlack   u_ex200903.log             u_ex201231.log             u_ex210309.log
u_ex191028.log                u_ex200522.log             u_ex200903.log.FileSlack   u_ex201231.log.FileSlack   u_ex210309.log.FileSlack
u_ex191029.log                u_ex200522.log.FileSlack   u_ex200924.log             u_ex210104.log             u_ex210310.log
u_ex191030.log                u_ex200526.log             u_ex200924.log.FileSlack   u_ex210105.log             u_ex210310.log.FileSlack
u_ex191031.log                u_ex200526.log.FileSlack   u_ex200929.log             u_ex210105.log.FileSlack   u_ex210311.log
u_ex191101.log                u_ex200527.log             u_ex200930.log             u_ex210106.log             u_ex210311.log.FileSlack
u_ex191104.log                u_ex200527.log.FileSlack   u_ex200930.log.FileSlack   u_ex210106.log.FileSlack   u_ex210312.log
u_ex191105.log                u_ex200528.log             u_ex201001.log             u_ex210107.log             u_ex210315.log
u_ex191105.log.FileSlack      u_ex200528.log.FileSlack   u_ex201008.log             u_ex210107.log.FileSlack   u_ex210315.log.FileSlack
u_ex191106.log                u_ex200601.log             u_ex201008.log.FileSlack   u_ex210108.log             u_ex210318.log
u_ex191107.log                u_ex200602.log             u_ex201019.log             u_ex210108.log.FileSlack   u_ex210324.log
u_ex191114.log                u_ex200603.log             u_ex201023.log             u_ex210111.log             u_ex210324.log.FileSlack
u_ex191115.log                u_ex200611.log             u_ex201023.log.FileSlack   u_ex210112.log             u_ex210329.log
u_ex191126.log                u_ex200611.log.FileSlack   u_ex201026.log             u_ex210113.log             u_ex210330.log
u_ex191126.log.FileSlack      u_ex200612.log             u_ex201026.log.FileSlack   u_ex210113.log.FileSlack   u_ex210331.log
u_ex200122.log                u_ex200612.log.FileSlack   u_ex201028.log             u_ex210114.log             u_ex210402.log
u_ex200122.log.FileSlack      u_ex200616.log             u_ex201029.log             u_ex210114.log.FileSlack   u_ex210402.log.FileSlack
u_ex200124.log                u_ex200616.log.FileSlack   u_ex201029.log.FileSlack   u_ex210115.log             u_ex210405.log
u_ex200124.log.FileSlack      u_ex200617.log             u_ex201102.log             u_ex210205.log             u_ex210405.log.FileSlack
u_ex200127.log                u_ex200618.log             u_ex201103.log             u_ex210205.log.FileSlack   u_ex210406.log
u_ex200131.log                u_ex200623.log             u_ex201109.log             u_ex210208.log             u_ex210406.log.FileSlack
u_ex200224.log                u_ex200623.log.FileSlack   u_ex201110.log             u_ex210208.log.FileSlack   u_ex210407.log
u_ex200226.log                u_ex200624.log             u_ex201113.log             u_ex210209.log             u_ex210407.log.FileSlack
u_ex200227.log                u_ex200624.log.FileSlack   u_ex201113.log.FileSlack   u_ex210209.log.FileSlack   u_ex210409.log
u_ex200228.log                u_ex200625.log             u_ex201120.log             u_ex210210.log             u_ex210409.log.FileSlack
u_ex200302.log                u_ex200629.log             u_ex201123.log             u_ex210210.log.FileSlack   u_ex210412.log
```

```
Cursor pos = 0
Selected: 0  EMSSERVER.E01/Partition 2 [95284MB]/OS [NTFS]/[root]/inetpub/logs/LogFiles/W3SVC1
```

Figure 9 - EMS Server (5.13) Web Server Log Files After



```
File List
u_ex210427.log
u_ex210427.log.FileSlack
u_ex210525.log
u_ex210525.log.FileSlack
u_ex210526.log
```

```
Cursor pos = 0
Selected: 0  EMSSERVER_v2.E01/Partition 4 [95274MB]/EMS [NTFS]/[root]/inetpub/logs/LogFiles/W3SVC1
```

Prior to the Dominion update, there were 240 log files in this folder. After the update, there are only 3 log files showing and 3 (partial) remnants of previously used log files in File Slack space.

A web server provides information to external web clients (via "web browser" software) using the HyperText Transfer Protocol (HTTP). This information can include both read and write access to databases and static presentation of information.

Some software system designs utilize an Ethernet network interface that is essentially an internal connection to itself, known as a *loopback* interface. Thus the presence of a Web Server, by itself, does not indicate a connection to an external ethernet interface. However, such an external connection may be indicated by the data within web server logs, which are stored by default in Microsoft operating systems with Microsoft Internet Information Services (IIS) installed, in a “logs” subfolder to the “inetpub” folder. That log data would include information regarding what web pages and data were accessed and whether it was accessed from within the server (loopback) or via an external network connection.

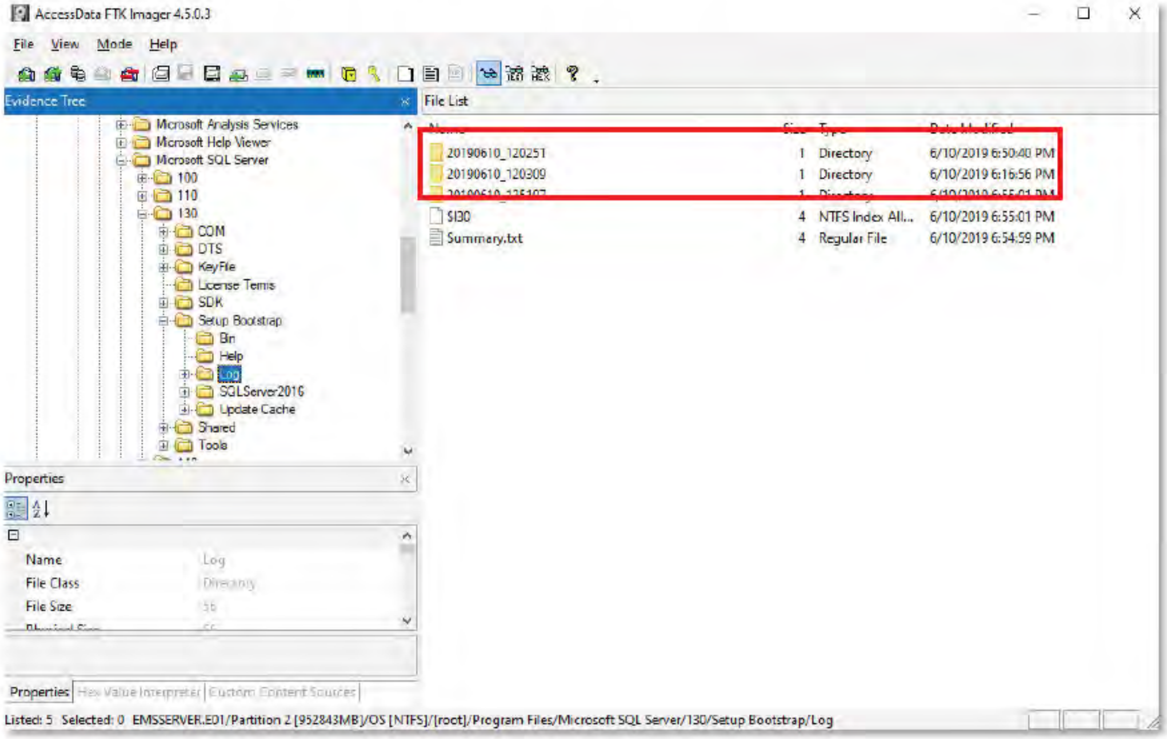
In these before and after views of the same web server directories, it is clear that the web server logs have been destroyed by or during the Dominion/CO Secretary of State DVS D-Suite 5.13 modification.

This log data is required to verify that the election system was not accessed by an external, unauthorized device, but due to the specific and unusual installation method for a critical computing system, chosen by Dominion Voting Systems and endorsed by the CO Secretary of State, these critical data files with election-related data have clearly been destroyed on the Mesa County EMS Standard Server.

Server Microsoft SQL Server Installation Log Files Missing

Purpose: *The Database Management System that is used to hold actual ELECTION DATA – votes from each ballot. These log files contain information detailing the installation events of SQL Server.*

Figure 10 - EMS Server (5.11-CO) MS SQL Server Installation Log Files Before



AccessData FTK Imager 4.5.0.3
File View Mode Help
Evidence Tree
File List
Properties
Properties | Hex Value Interpreter | Custom Content Sources

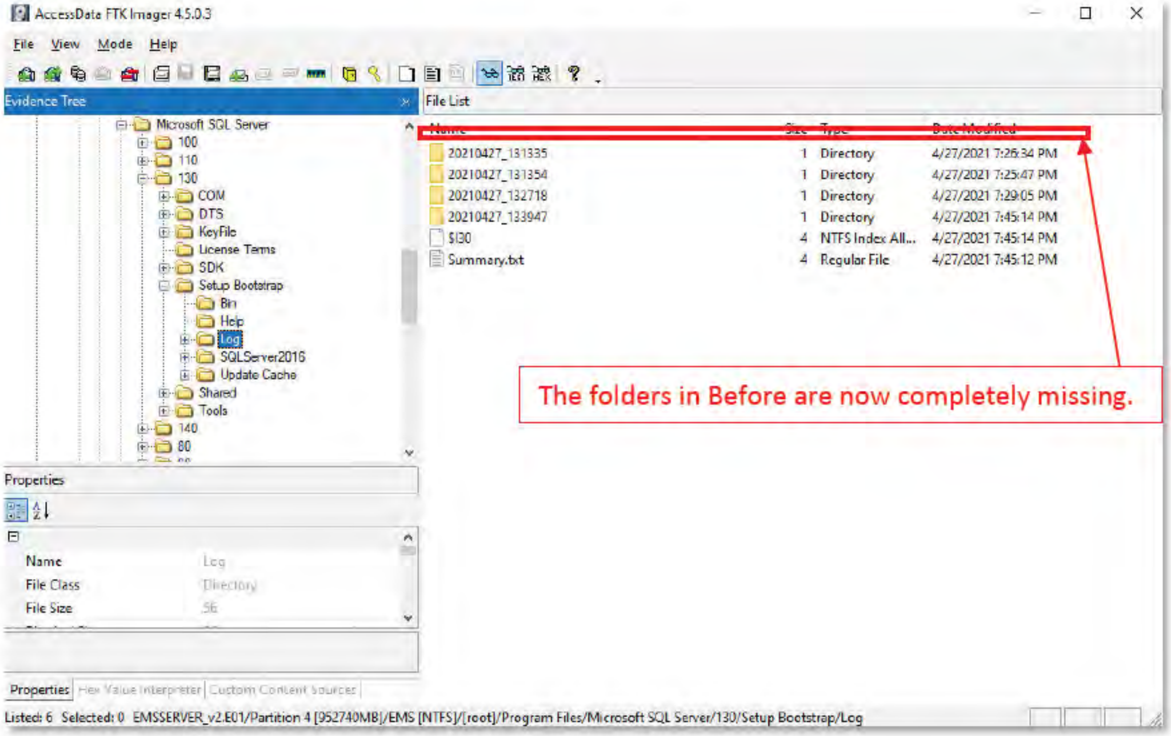
```
Microsoft Analysis Services
Microsoft Help Viewer
Microsoft SQL Server
  100
  110
  130
    COM
    DTS
    KeyFile
    License Terms
    SDK
    Setup Bootstrap
      Bin
      Help
      Log
      SQLServer2016
      Update Cache
    Shared
    Tools
```

Name	Size	Type	Date Modified
20190610_120251	1	Directory	6/10/2019 6:50:40 PM
20190610_120309	1	Directory	6/10/2019 6:16:56 PM
20190610_125107	1	Directory	6/10/2019 6:55:01 PM
$I30	4	NTFS Index All...	6/10/2019 6:55:01 PM
Summary.txt	4	Regular File	6/10/2019 6:54:59 PM

Name	Log
File Class	Directory
File Size	56

Listed: 5 Selected: 0 EMSSERVER.E01/Partition 2 [952843MB]/OS [NTFS]/[root]/Program Files/Microsoft SQL Server/130/Setup Bootstrap/Log

Figure 11 - EMS Server (5.13) MS SQL Server Installation Log Files After



AccessData FTK Imager 4.5.0.3
File View Mode Help
Evidence Tree
File List
Properties
Properties | Hex Value Interpreter | Custom Content Sources

```
Microsoft SQL Server
  100
  110
  130
    COM
    DTS
    KeyFile
    License Terms
    SDK
    Setup Bootstrap
      Bin
      Help
      Log
      SQLServer2016
      Update Cache
    Shared
    Tools
  140
  80
```

Name	Size	Type	Date Modified
20210427_131335	1	Directory	4/27/2021 7:26:34 PM
20210427_131354	1	Directory	4/27/2021 7:25:47 PM
20210427_132718	1	Directory	4/27/2021 7:29:05 PM
20210427_133947	1	Directory	4/27/2021 7:45:14 PM
$I30	4	NTFS Index All...	4/27/2021 7:45:14 PM
Summary.txt	4	Regular File	4/27/2021 7:45:12 PM

Name	Log
File Class	Directory
File Size	56

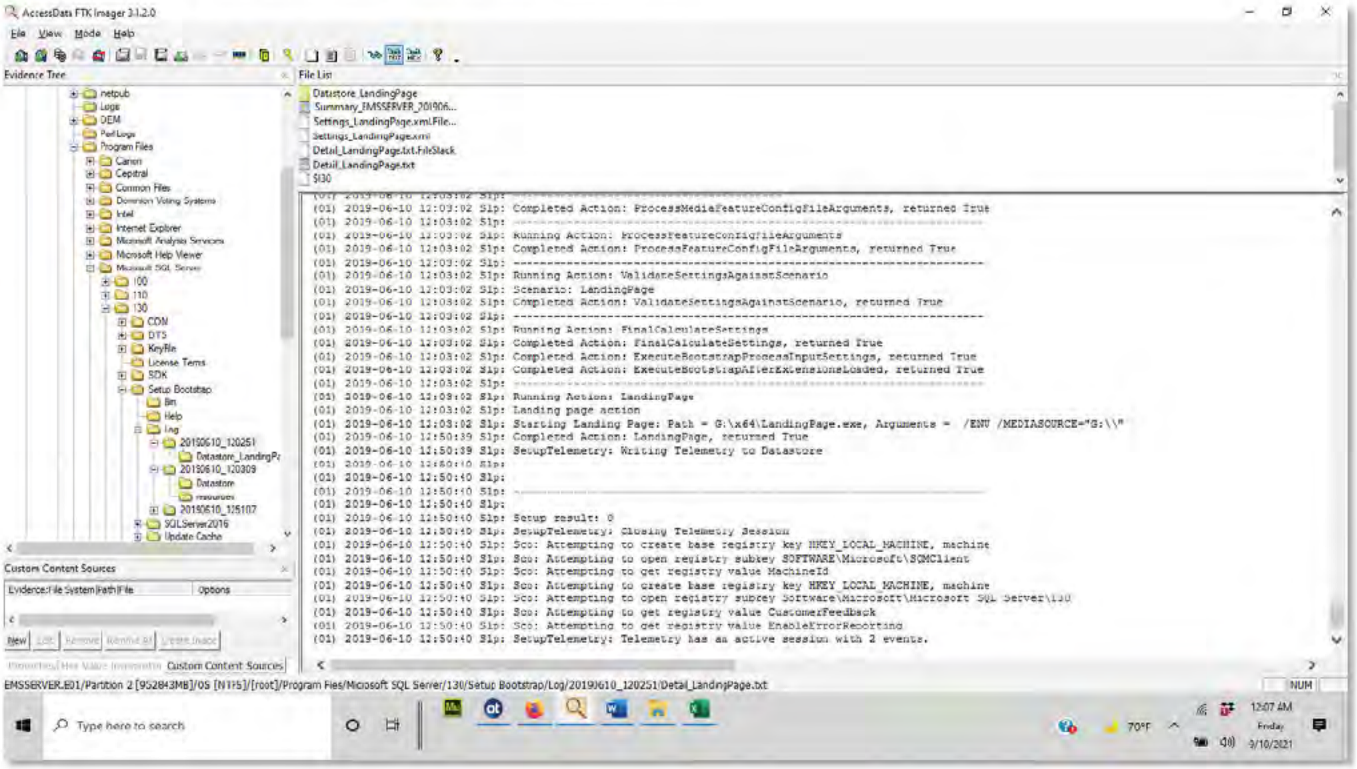
Listed: 6 Selected: 0 EMSSERVER_v2.E01/Partition 4 [952740MB]/EMS [NTFS]/[root]/Program Files/Microsoft SQL Server/130/Setup Bootstrap/Log

The folders in Before are now completely missing.

These log files were created by installing the SQL Server Database Management System software and contain data regarding the Initial installation of the software. In a full forensic investigation, these data are part of the information that investigators require to determine a baseline from which can be determined what changes were made, by whom, when the changes were made, and much more on a system with properly configured log recording. Therefore, these data are Election Related as they document not only the configuration but its changes and are relevant to the Integrity of the election.

Figure 12 is an example of log content from the initial software setup. It tells us what (Microsoft) software executes, where data is stored (the G: drive), and it shows us what Registry values have been set during the installation. These are valuable should an investigation of an illegal computer intrusion occur, as they provide a record of the initial configuration during such an investigation.

Figure 12 - Example of Log File Content from EMS Server (5.11-CO) Before



Datastore_LandingPage
Summary_EMSSERVER_201906...
Settings_LandingPage.xml.File...
Settings_LandingPage.xml
Detail_LandingPage.txt.FileSlack
Detail_LandingPage.txt
$I30

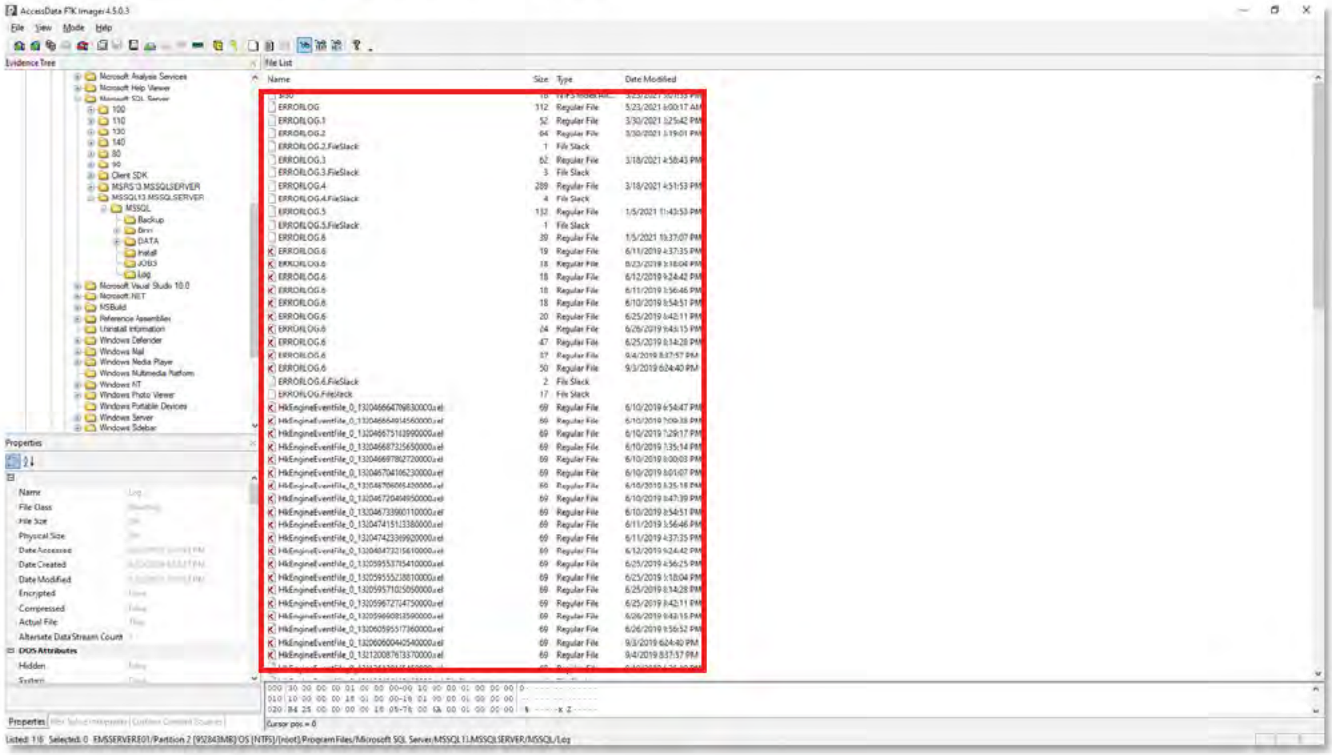
```
(01) 2019-06-10 12:03:02 Slp: Completed Action: ProcessMediaFeatureConfigFileArguments, returned True
(01) 2019-06-10 12:03:02 Slp: ----------------------------------------------------------------------
(01) 2019-06-10 12:03:02 Slp: Running Action: ProcessFeatureConfigFileArguments
(01) 2019-06-10 12:03:02 Slp: Completed Action: ProcessFeatureConfigFileArguments, returned True
(01) 2019-06-10 12:03:02 Slp: ----------------------------------------------------------------------
(01) 2019-06-10 12:03:02 Slp: Running Action: ValidateSettingsAgainstScenario
(01) 2019-06-10 12:03:02 Slp: Scenario: LandingPage
(01) 2019-06-10 12:03:02 Slp: Completed Action: ValidateSettingsAgainstScenario, returned True
(01) 2019-06-10 12:03:02 Slp: ----------------------------------------------------------------------
(01) 2019-06-10 12:03:02 Slp: Running Action: FinalCalculateSettings
(01) 2019-06-10 12:03:02 Slp: Completed Action: FinalCalculateSettings, returned True
(01) 2019-06-10 12:03:02 Slp: Completed Action: ExecuteBootstrapProcessInputSettings, returned True
(01) 2019-06-10 12:03:02 Slp: Completed Action: ExecuteBootstrapAfterExtensionsLoaded, returned True
(01) 2019-06-10 12:03:02 Slp: ----------------------------------------------------------------------
(01) 2019-06-10 12:03:02 Slp: Running Action: LandingPage
(01) 2019-06-10 12:03:02 Slp: Landing page action
(01) 2019-06-10 12:03:02 Slp: Starting Landing Page: Path = G:\x64\LandingPage.exe, Arguments =  /ENU /MEDIASOURCE="G:\\"
(01) 2019-06-10 12:50:39 Slp: Completed Action: LandingPage, returned True
(01) 2019-06-10 12:50:39 Slp: SetupTelemetry: Writing Telemetry to Datastore
(01) 2019-06-10 12:50:40 Slp:
(01) 2019-06-10 12:50:40 Slp:
(01) 2019-06-10 12:50:40 Slp: ----------------------------------------------------------------------
(01) 2019-06-10 12:50:40 Slp:
(01) 2019-06-10 12:50:40 Slp: Setup result: 0
(01) 2019-06-10 12:50:40 Slp: SetupTelemetry: Closing Telemetry Session
(01) 2019-06-10 12:50:40 Slp: Sco: Attempting to create base registry key HKEY_LOCAL_MACHINE, machine
(01) 2019-06-10 12:50:40 Slp: Sco: Attempting to open registry subkey SOFTWARE\Microsoft\SQMClient
(01) 2019-06-10 12:50:40 Slp: Sco: Attempting to get registry value MachineId
(01) 2019-06-10 12:50:40 Slp: Sco: Attempting to create base registry key HKEY_LOCAL_MACHINE, machine
(01) 2019-06-10 12:50:40 Slp: Sco: Attempting to open registry subkey Software\Microsoft\Microsoft SQL Server\130
(01) 2019-06-10 12:50:40 Slp: Sco: Attempting to get registry value CustomerFeedback
(01) 2019-06-10 12:50:40 Slp: Sco: Attempting to get registry value EnableErrorReporting
(01) 2019-06-10 12:50:40 Slp: SetupTelemetry: Telemetry has an active session with 2 events.
```

EMSSERVER.E01/Partition 2 [952843MB]/OS [NTFS]/[root]/Program Files/Microsoft SQL Server/130/Setup Bootstrap/Log/20190610_120251/Detail_LandingPage.txt

Server Microsoft SQL Server Log Files Missing

Purpose: *These log files keep track of events that occur within the SQL Server that manages the election databases.*

Figure 13 - EMS Server (5.11-CO) SQL Server Log Files Before



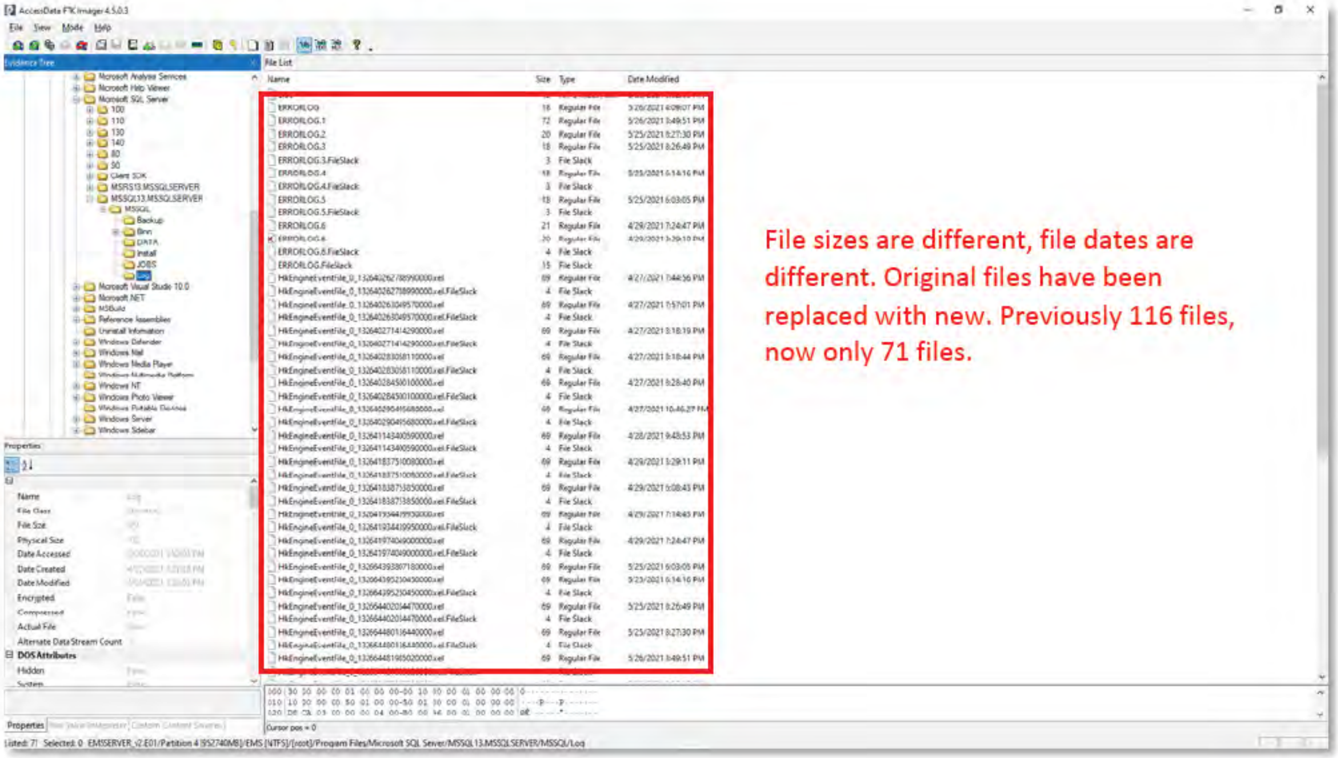
Name	Size	Type	Date Modified
ERRORLOG	112	Regular File	5/23/2021 6:00:17 AM
ERRORLOG.1	52	Regular File	3/30/2021 3:25:42 PM
ERRORLOG.2	64	Regular File	3/30/2021 3:19:01 PM
ERRORLOG.2.FileSlack	1	File Slack	
ERRORLOG.3	62	Regular File	3/18/2021 4:58:43 PM
ERRORLOG.3.FileSlack	3	File Slack	
ERRORLOG.4	289	Regular File	3/18/2021 4:51:53 PM
ERRORLOG.4.FileSlack	4	File Slack	
ERRORLOG.5	132	Regular File	1/5/2021 11:43:53 PM
ERRORLOG.5.FileSlack	1	File Slack	
ERRORLOG.6	39	Regular File	1/5/2021 10:37:07 PM
ERRORLOG.6	19	Regular File	6/11/2019 4:37:35 PM
ERRORLOG.6	18	Regular File	6/23/2019 3:18:04 PM
ERRORLOG.6	18	Regular File	6/12/2019 9:24:42 PM
ERRORLOG.6	18	Regular File	6/11/2019 3:56:46 PM
ERRORLOG.6	18	Regular File	6/10/2019 8:54:51 PM
ERRORLOG.6	20	Regular File	6/25/2019 6:42:11 PM
ERRORLOG.6	24	Regular File	6/26/2019 9:43:15 PM
ERRORLOG.6	47	Regular File	6/25/2019 8:14:28 PM
ERRORLOG.6	37	Regular File	9/4/2019 8:37:57 PM
ERRORLOG.6	50	Regular File	9/3/2019 6:24:40 PM
ERRORLOG.6.FileSlack	2	File Slack	
ERRORLOG.FileSlack	17	File Slack	
HkEngineEventFile_0_132046664709830000.xel	69	Regular File	6/10/2019 6:54:47 PM
HkEngineEventFile_0_132046664914560000.xel	69	Regular File	6/10/2019 7:09:38 PM
HkEngineEventFile_0_132046675143990000.xel	69	Regular File	6/10/2019 7:29:17 PM
HkEngineEventFile_0_132046687325650000.xel	69	Regular File	6/10/2019 7:35:14 PM
HkEngineEventFile_0_132046697802720000.xel	69	Regular File	6/10/2019 8:00:03 PM
HkEngineEventFile_0_132046704106230000.xel	69	Regular File	6/10/2019 8:01:07 PM
HkEngineEventFile_0_132046706065430000.xel	69	Regular File	6/10/2019 8:35:18 PM
HkEngineEventFile_0_132046720404950000.xel	69	Regular File	6/10/2019 8:47:39 PM
HkEngineEventFile_0_132046733980110000.xel	69	Regular File	6/10/2019 8:54:51 PM
HkEngineEventFile_0_132047415133380000.xel	69	Regular File	6/11/2019 3:56:46 PM
HkEngineEventFile_0_132047423369920000.xel	69	Regular File	6/11/2019 4:37:35 PM
HkEngineEventFile_0_132048473215610000.xel	69	Regular File	6/12/2019 9:24:42 PM
HkEngineEventFile_0_132059553715410000.xel	69	Regular File	6/25/2019 4:56:25 PM
HkEngineEventFile_0_132059555238810000.xel	69	Regular File	6/25/2019 5:18:04 PM
HkEngineEventFile_0_132059571025050000.xel	69	Regular File	6/25/2019 8:14:28 PM
HkEngineEventFile_0_132059672704750000.xel	69	Regular File	6/25/2019 8:42:11 PM
HkEngineEventFile_0_132059690813590000.xel	69	Regular File	6/26/2019 9:43:15 PM
HkEngineEventFile_0_132060595517360000.xel	69	Regular File	6/26/2019 9:56:52 PM
HkEngineEventFile_0_132060600440540000.xel	69	Regular File	9/3/2019 6:24:40 PM
HkEngineEventFile_0_132120087613370000.xel	69	Regular File	9/4/2019 8:37:57 PM

```
000 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00 0
010 10 00 00 00 18 01 00 00-18 01 00 00 01 00 00 00
020 84 25 00 00 00 00 18 05-78 00 5A 00 01 00 00 00 % x Z
```

Cursor pos = 0

Listed: 116 Selected: 0 EMSSERVERE01/Partition 2 [952843MB]/OS [NTFS]/[root]/Program Files/Microsoft SQL Server/MSSQL11.MSSQLSERVER/MSSQL/Log

Figure 14 - EMS Server (5.13) SQL Server Log Files After



Name	Size	Type	Date Modified
ERRORLOG	18	Regular File	5/26/2021 4:09:07 PM
ERRORLOG.1	72	Regular File	5/26/2021 3:49:51 PM
ERRORLOG.2	20	Regular File	5/25/2021 8:27:30 PM
ERRORLOG.3	18	Regular File	5/25/2021 8:26:49 PM
ERRORLOG.3.FileSlack	3	File Slack	
ERRORLOG.4	18	Regular File	5/25/2021 6:14:16 PM
ERRORLOG.4.FileSlack	3	File Slack	
ERRORLOG.5	18	Regular File	5/25/2021 6:03:05 PM
ERRORLOG.5.FileSlack	3	File Slack	
ERRORLOG.6	21	Regular File	4/29/2021 7:24:47 PM
ERRORLOG.6	20	Regular File	4/29/2021 3:29:10 PM
ERRORLOG.6.FileSlack	4	File Slack	
ERRORLOG.FileSlack	15	File Slack	
HkEngineEventFile_0_132640262788990000.xel	69	Regular File	4/27/2021 7:44:56 PM
HkEngineEventFile_0_132640262788990000.xel.FileSlack	4	File Slack	
HkEngineEventFile_0_132640263049570000.xel	69	Regular File	4/27/2021 7:57:01 PM
HkEngineEventFile_0_132640263049570000.xel.FileSlack	4	File Slack	
HkEngineEventFile_0_132640271414290000.xel	69	Regular File	4/27/2021 8:18:19 PM
HkEngineEventFile_0_132640271414290000.xel.FileSlack	4	File Slack	
HkEngineEventFile_0_132640283058110000.xel	69	Regular File	4/27/2021 8:18:44 PM
HkEngineEventFile_0_132640283058110000.xel.FileSlack	4	File Slack	
HkEngineEventFile_0_132640284530100000.xel	69	Regular File	4/27/2021 8:28:40 PM
HkEngineEventFile_0_132640284530100000.xel.FileSlack	4	File Slack	
HkEngineEventFile_0_132640290495680000.xel	69	Regular File	4/27/2021 10:46:27 PM
HkEngineEventFile_0_132640290495680000.xel.FileSlack	4	File Slack	
HkEngineEventFile_0_132641143400590000.xel	69	Regular File	4/28/2021 9:48:53 PM
HkEngineEventFile_0_132641143400590000.xel.FileSlack	4	File Slack	
HkEngineEventFile_0_132641837510080000.xel	69	Regular File	4/29/2021 3:29:11 PM
HkEngineEventFile_0_132641837510080000.xel.FileSlack	4	File Slack	
HkEngineEventFile_0_132641838713850000.xel	69	Regular File	4/29/2021 5:08:43 PM
HkEngineEventFile_0_132641838713850000.xel.FileSlack	4	File Slack	
HkEngineEventFile_0_132641934419950000.xel	69	Regular File	4/29/2021 7:14:43 PM
HkEngineEventFile_0_132641934419950000.xel.FileSlack	4	File Slack	
HkEngineEventFile_0_132641974049000000.xel	69	Regular File	4/29/2021 7:24:47 PM
HkEngineEventFile_0_132641974049000000.xel.FileSlack	4	File Slack	
HkEngineEventFile_0_132664393807180000.xel	69	Regular File	5/25/2021 6:03:05 PM
HkEngineEventFile_0_132664395230450000.xel	69	Regular File	5/25/2021 6:14:16 PM
HkEngineEventFile_0_132664395230450000.xel.FileSlack	4	File Slack	
HkEngineEventFile_0_132664402014470000.xel	69	Regular File	5/25/2021 8:26:49 PM
HkEngineEventFile_0_132664402014470000.xel.FileSlack	4	File Slack	
HkEngineEventFile_0_132664480136440000.xel	69	Regular File	5/25/2021 8:27:30 PM
HkEngineEventFile_0_132664480136440000.xel.FileSlack	4	File Slack	
HkEngineEventFile_0_132664481905020000.xel	69	Regular File	5/26/2021 3:49:51 PM

```
000 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00 0
010 10 00 00 00 50 01 00 00-50 01 00 00 01 00 00 00 P P
020 D8 CA 03 00 00 00 04 00-80 00 46 00 01 00 00 00 ØÊ *
```

Cursor pos = 0

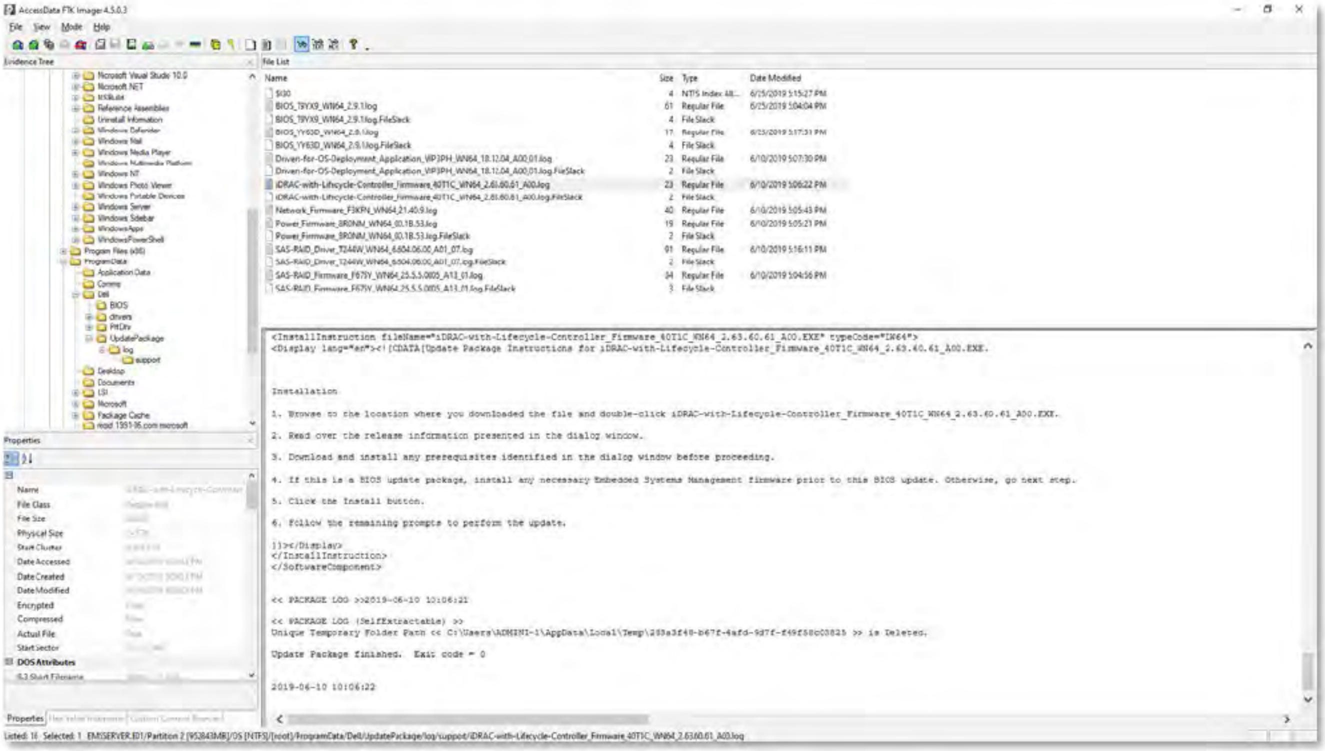
Listed: 71 Selected: 0 EMSSERVER_v2.E01/Partition 4 [952740MB]/EMS [NTFS]/[root]/Progam Files/Microsoft SQL Server/MSSQL13.MSSQLSERVER/MSSQL/Log

File sizes are different, file dates are different. Original files have been replaced with new. Previously 116 files, now only 71 files.

EMS Server Dell Server Updates Missing

Purpose: *These log files track installation of updates made to the various components of the servers, including updates to software for a remote-access card.*

Figure 15 - EMS Server (5.11-CO) Dell Server Update Files Before

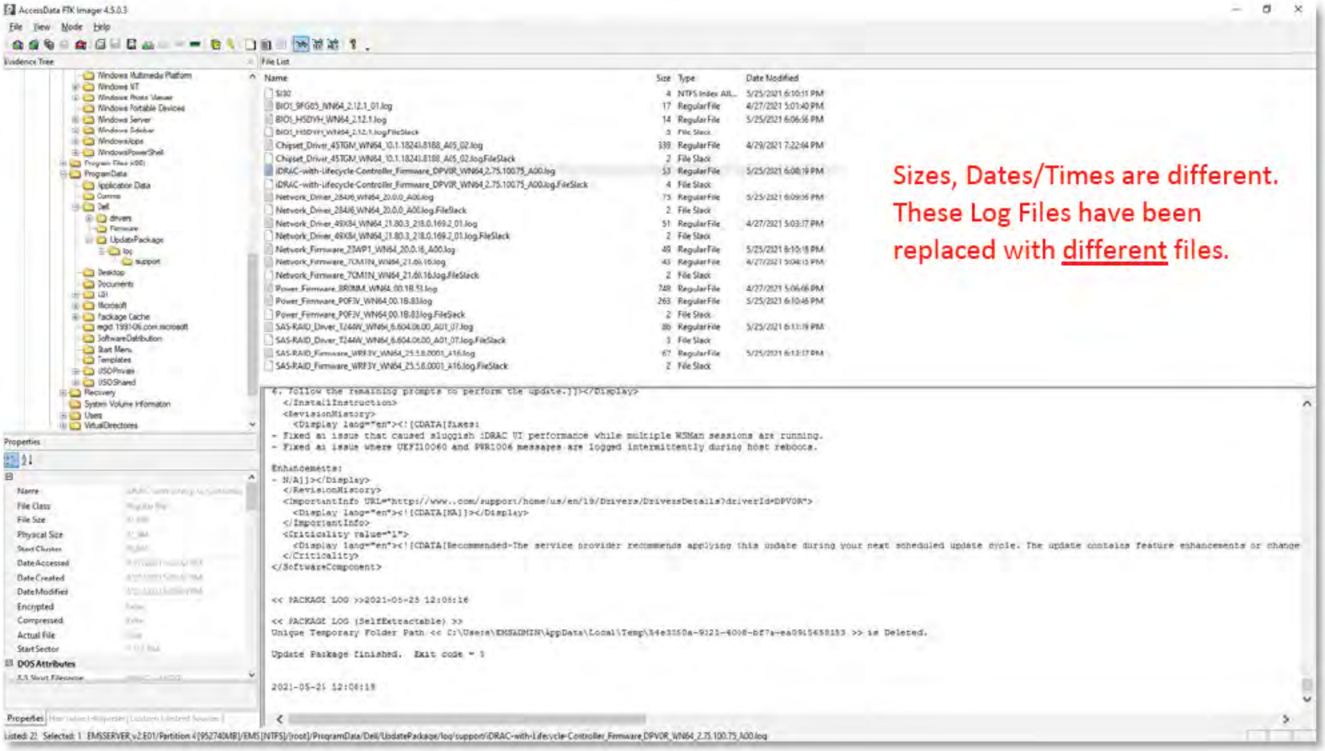


```
Name                                                                          Size  Type             Date Modified
$I30                                                                             4  NTFS Index All...  6/25/2019 5:15:27 PM
BIOS_T9YX9_WN64_2.9.1.log                                                       61  Regular File     6/25/2019 5:04:04 PM
BIOS_T9YX9_WN64_2.9.1.log.FileSlack                                              4  File Slack
BIOS_YY63D_WN64_2.9.1.log                                                       17  Regular File     6/25/2019 5:17:31 PM
BIOS_YY63D_WN64_2.9.1.log.FileSlack                                              4  File Slack
Driven-for-OS-Deployment_Application_VP3PH_WN64_18.12.04_A00.01.log             23  Regular File     6/10/2019 5:07:30 PM
Driven-for-OS-Deployment_Application_VP3PH_WN64_18.12.04_A00.01.log.FileSlack    2  File Slack
iDRAC-with-Lifecycle-Controller_Firmware_40T1C_WN64_2.63.60.61_A00.log          23  Regular File     6/10/2019 5:06:22 PM
iDRAC-with-Lifecycle-Controller_Firmware_40T1C_WN64_2.63.60.61_A00.log.FileSlack  2  File Slack
Network_Firmware_F3KPN_WN64_21.40.9.log                                         40  Regular File     6/10/2019 5:05:43 PM
Power_Firmware_8R0NM_WN64_00.1B.53.log                                          19  Regular File     6/10/2019 5:05:21 PM
Power_Firmware_8R0NM_WN64_00.1B.53.log.FileSlack                                 2  File Slack
SAS-RAID_Driver_T244W_WN64_6.604.06.00_A01_07.log                               91  Regular File     6/10/2019 5:16:11 PM
SAS-RAID_Driver_T244W_WN64_6.604.06.00_A01_07.log.FileSlack                      2  File Slack
SAS-RAID_Firmware_F675Y_WN64_25.5.5.0005_A13_01.log                             34  Regular File     6/10/2019 5:04:56 PM
SAS-RAID_Firmware_F675Y_WN64_25.5.5.0005_A13_01.log.FileSlack                    3  File Slack
```

```
<InstallInstruction fileName="iDRAC-with-Lifecycle-Controller_Firmware_40T1C_WN64_2.63.60.61_A00.EXE" typeCode="IW64">
<Display lang="en"><![CDATA[Update Package Instructions for iDRAC-with-Lifecycle-Controller_Firmware_40T1C_WN64_2.63.60.61_A00.EXE.


Installation

1. Browse to the location where you downloaded the file and double-click iDRAC-with-Lifecycle-Controller_Firmware_40T1C_WN64_2.63.60.61_A00.EXE.

2. Read over the release information presented in the dialog window.

3. Download and install any prerequisites identified in the dialog window before proceeding.

4. If this is a BIOS update package, install any necessary Embedded Systems Management firmware prior to this BIOS update. Otherwise, go next step.

5. Click the Install button.

6. Follow the remaining prompts to perform the update.

]]></Display>
</InstallInstruction>
</SoftwareComponent>


<< PACKAGE LOG >>2019-06-10 10:06:21

<< PACKAGE LOG (SelfExtractable) >>
Unique Temporary Folder Path << C:\Users\ADMINI~1\AppData\Local\Temp\283a3f48-b67f-4afd-9d7f-f49f58c03825 >> is Deleted.

Update Package finished.  Exit code = 0


2019-06-10 10:06:22
```

```
Listed: 16  Selected: 1  EMSSERVER.E01/Partition 2 [952843MB]/OS [NTFS]/[root]/ProgramData/Dell/UpdatePackage/log/support/iDRAC-with-Lifecycle-Controller_Firmware_40T1C_WN64_2.63.60.61_A00.log
```

Figure 16 - EMS Server (5.13) Dell Server Update Files After



```
Name                                                                          Size  Type             Date Modified
$I30                                                                             4  NTFS Index All...  5/25/2021 6:10:11 PM
BIOS_9FG05_WN64_2.12.1_01.log                                                   17  Regular File     4/27/2021 5:01:40 PM
BIOS_H5DVH_WN64_2.12.1.log                                                      14  Regular File     5/25/2021 6:06:56 PM
BIOS_H5DVH_WN64_2.12.1.log.FileSlack                                             3  File Slack
Chipset_Driver_45TGM_WN64_10.1.18243.8188_A05_02.log                           339  Regular File     4/29/2021 7:22:04 PM
Chipset_Driver_45TGM_WN64_10.1.18243.8188_A05_02.log.FileSlack                   2  File Slack
iDRAC-with-Lifecycle-Controller_Firmware_DPV0R_WN64_2.75.100.75_A00.log         53  Regular File     5/25/2021 6:08:19 PM
iDRAC-with-Lifecycle-Controller_Firmware_DPV0R_WN64_2.75.100.75_A00.log.FileSlack  4  File Slack
Network_Driver_2846_WN64_20.0.0_A00.log                                         75  Regular File     5/25/2021 6:09:36 PM
Network_Driver_2846_WN64_20.0.0_A00.log.FileSlack                                2  File Slack
Network_Driver_49X84_WN64_21.80.3_218.0.169.2_01.log                            51  Regular File     4/27/2021 5:03:17 PM
Network_Driver_49X84_WN64_21.80.3_218.0.169.2_01.log.FileSlack                   2  File Slack
Network_Firmware_23WP1_WN64_20.0.16_A00.log                                     49  Regular File     5/25/2021 6:10:18 PM
Network_Firmware_7CM1N_WN64_21.60.16.log                                        43  Regular File     4/27/2021 5:04:15 PM
Network_Firmware_7CM1N_WN64_21.60.16.log.FileSlack                               2  File Slack
Power_Firmware_8R0NM_WN64_00.1B.53.log                                         748  Regular File     4/27/2021 5:06:06 PM
Power_Firmware_P0F3V_WN64_00.1B.83.log                                         263  Regular File     5/25/2021 6:10:46 PM
Power_Firmware_P0F3V_WN64_00.1B.83.log.FileSlack                                 2  File Slack
SAS-RAID_Driver_T244W_WN64_6.604.06.00_A01_07.log                               86  Regular File     5/25/2021 6:11:19 PM
SAS-RAID_Driver_T244W_WN64_6.604.06.00_A01_07.log.FileSlack                      3  File Slack
SAS-RAID_Firmware_WRF3Y_WN64_25.5.8.0001_A16.log                                67  Regular File     5/25/2021 6:13:17 PM
SAS-RAID_Firmware_WRF3Y_WN64_25.5.8.0001_A16.log.FileSlack                       2  File Slack
```

```
4. Follow the remaining prompts to perform the update.]]></Display>
  </InstallInstruction>
  <RevisionHistory>
    <Display lang="en"><![CDATA[fixes:
- Fixed an issue that caused sluggish iDRAC UI performance while multiple WSMan sessions are running.
- Fixed an issue where UEFI0060 and PWR1006 messages are logged intermittently during host reboots.

Enhancements:
- N/A]]></Display>
  </RevisionHistory>
  <ImportantInfo URL="http://www..com/support/home/us/en/19/Drivers/DriversDetails?driverId=DPV0R">
    <Display lang="en"><![CDATA[NA]]></Display>
  </ImportantInfo>
  <Criticality value="1">
    <Display lang="en"><![CDATA[Recommended-The service provider recommends applying this update during your next scheduled update cycle. The update contains feature enhancements or change
  </Criticality>
</SoftwareComponent>


<< PACKAGE LOG >>2021-05-25 12:08:16

<< PACKAGE LOG (SelfExtractable) >>
Unique Temporary Folder Path << C:\Users\EMSADMIN\AppData\Local\Temp\54e3350a-9121-4008-bf7a-ea0915658153 >> is Deleted.

Update Package finished.  Exit code = 1


2021-05-25 12:08:18
```

```
Listed: 22  Selected: 1  EMSSERVER_v2.E01/Partition 4 [952740MB]/EMS [NTFS]/[root]/ProgramData/Dell/UpdatePackage/log/support/iDRAC-with-Lifecycle-Controller_Firmware_DPV0R_WN64_2.75.100.75_A00.log
```

Sizes, Dates/Times are different. These Log Files have been replaced with different files.

Several log files of great importance to an investigation are shown in Figure 16. The SAS RAID firmware and drivers logs tell us about the functionality of hard disk controllers (RAID is an acronym for Redundant Array of Independent Disks) and about this storage redundancy's physical capability. Network Firmware logs tell us which hardware devices were updated with new firmware, and the version allows us to trace back to its network (and possibly Internet) functionality. The application of iDRAC controller firmware may indicate the presence of a special hardware controller intended to permit complete remote control of the computer system. This iDRAC controller is often used when a data center must be located an inconvenient distance away from its owner and/or operators, or for example, when such a computer might be physically located at an Internet Service Provider's secure data center. The iDRAC controller permits a remote user to remotely turn on the power to the server, reboot it, access administrative control functions, and make changes to the server, *OUTSIDE THE CONTROL, or even the awareness, of the local computer operator and its operating system.* Among the changes possible via an IDRAC are changes to the BIOS (Basic I/O System) including those firmware settings that include the computer Clock, boot device order, which disks or other data storage devices are used to boot the computer, and some other computer capabilities.

Take note of what files remain following the update.

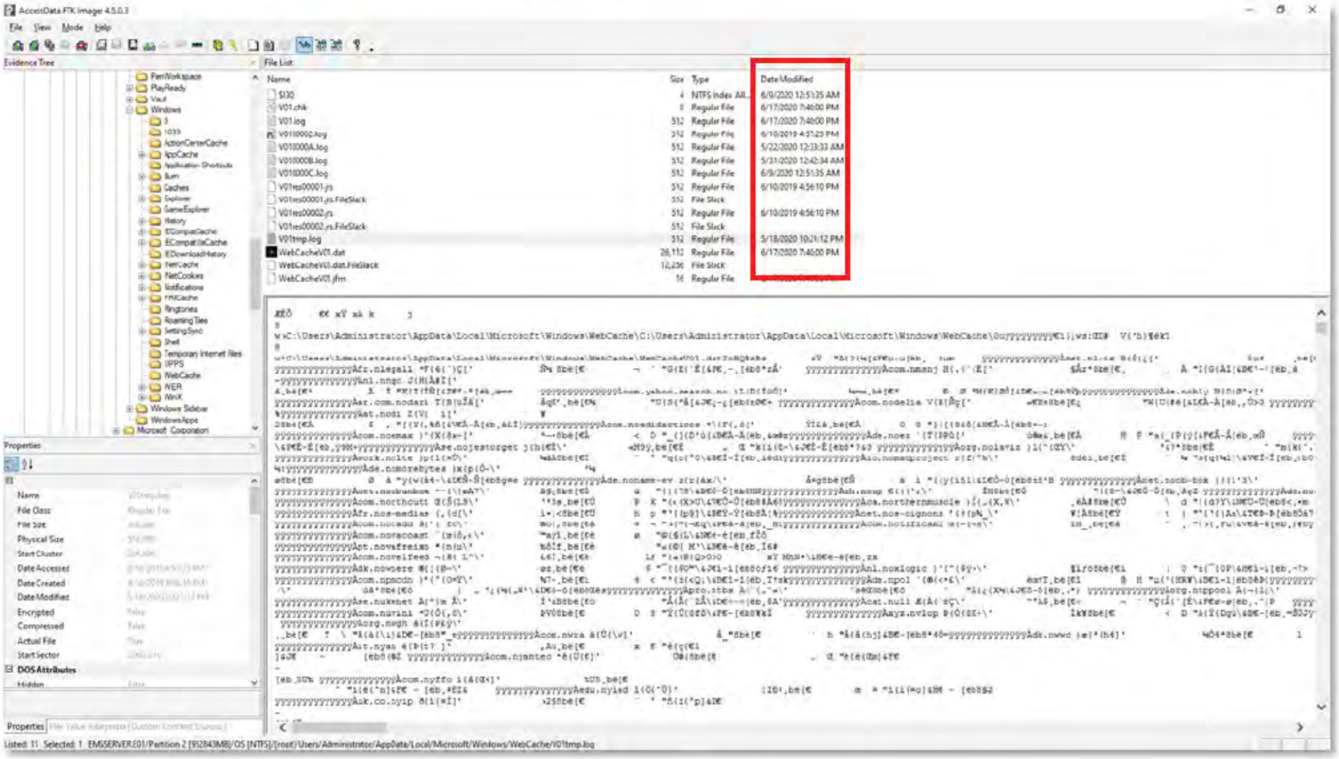
Not only are the files in an entirely different directory, but the file modification dates have changed, and more importantly, these logs are for DIFFERENT versions of the software, and the previous logs have been overwritten.

Physical examination of the EMS computer system is required to verify the presence or absence of an IDRAC controller, however it is highly irregular for update software to install updates to software for a hardware device that has not been installed.

Server 'Administrator' WebCache Log Files Overwritten

Purpose: *These log files store information about websites visited, files opened, etc.*

Figure 17 - EMS Server (5.11-CO) Administrator WebCache Log Files Before

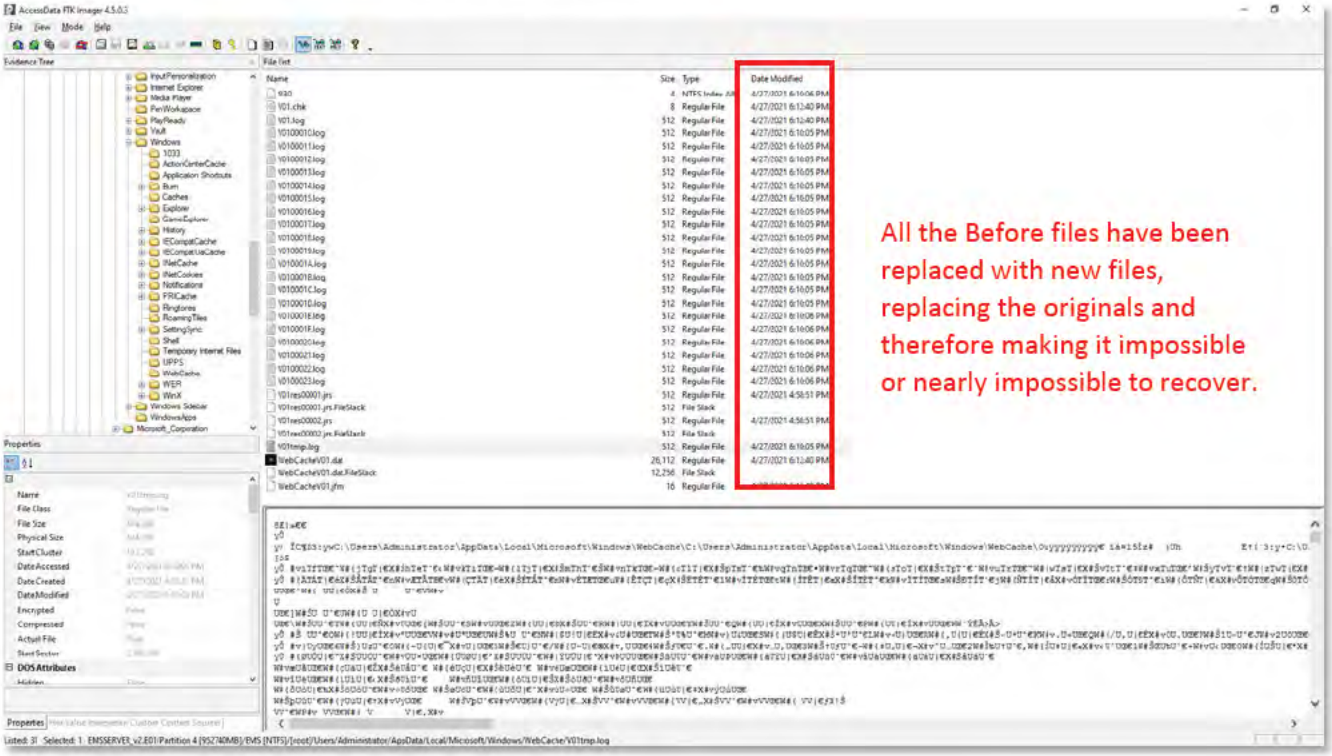


Name	Size	Type	Date Modified
$I30	4	NTFS Index All...	6/9/2020 12:51:35 AM
V01.chk	8	Regular File	6/17/2020 7:40:00 PM
V01.log	512	Regular File	6/17/2020 7:40:00 PM
V0100002.log	512	Regular File	6/10/2019 4:57:25 PM
V010000A.log	512	Regular File	5/22/2020 12:13:33 AM
V010000B.log	512	Regular File	5/31/2020 12:42:34 AM
V010000C.log	512	Regular File	6/9/2020 12:51:35 AM
V01res00001.jrs	512	Regular File	6/10/2019 4:56:10 PM
V01res00001.jrs.FileSlack	512	File Slack	
V01res00002.jrs	512	Regular File	6/10/2019 4:56:10 PM
V01res00002.jrs.FileSlack	512	File Slack	
V01tmp.log	512	Regular File	5/18/2020 10:21:12 PM
WebCacheV01.dat	26,112	Regular File	6/17/2020 7:40:00 PM
WebCacheV01.dat.FileSlack	12,256	File Slack	
WebCacheV01.jfm	16	Regular File	

```
w C:\Users\Administrator\AppData\Local\Microsoft\Windows\WebCache\C:\Users\Administrator\AppData\Local\Microsoft\Windows\WebCache\
```

Listed: 11 Selected: 1 EMSSERVER.E01/Partition 2 [912843MB]/OS [NTFS]/[root]/Users/Administrator/AppData/Local/Microsoft/Windows/WebCache/V01tmp.log

Figure 18 - EMS Server (5.13) Administrator WebCache Log Files After



Name	Size	Type	Date Modified
$I30	4	NTFS Index All...	4/27/2021 6:10:06 PM
V01.chk	8	Regular File	4/27/2021 6:12:40 PM
V01.log	512	Regular File	4/27/2021 6:12:40 PM
V0100010.log	512	Regular File	4/27/2021 6:10:05 PM
V0100011.log	512	Regular File	4/27/2021 6:10:05 PM
V0100012.log	512	Regular File	4/27/2021 6:10:05 PM
V0100013.log	512	Regular File	4/27/2021 6:10:05 PM
V0100014.log	512	Regular File	4/27/2021 6:10:05 PM
V0100015.log	512	Regular File	4/27/2021 6:10:05 PM
V0100016.log	512	Regular File	4/27/2021 6:10:05 PM
V0100017.log	512	Regular File	4/27/2021 6:10:05 PM
V0100018.log	512	Regular File	4/27/2021 6:10:05 PM
V0100019.log	512	Regular File	4/27/2021 6:10:05 PM
V010001A.log	512	Regular File	4/27/2021 6:10:05 PM
V010001B.log	512	Regular File	4/27/2021 6:10:05 PM
V010001C.log	512	Regular File	4/27/2021 6:10:05 PM
V010001D.log	512	Regular File	4/27/2021 6:10:05 PM
V010001E.log	512	Regular File	4/27/2021 6:10:06 PM
V010001F.log	512	Regular File	4/27/2021 6:10:06 PM
V0100020.log	512	Regular File	4/27/2021 6:10:06 PM
V0100021.log	512	Regular File	4/27/2021 6:10:06 PM
V0100022.log	512	Regular File	4/27/2021 6:10:06 PM
V0100023.log	512	Regular File	4/27/2021 6:10:06 PM
V01res00001.jrs	512	Regular File	4/27/2021 4:58:51 PM
V01res00001.jrs.FileSlack	512	File Slack	
V01res00002.jrs	512	Regular File	4/27/2021 4:58:51 PM
V01res00002.jrs.FileSlack	512	File Slack	
V01tmp.log	512	Regular File	4/27/2021 6:10:05 PM
WebCacheV01.dat	26,112	Regular File	4/27/2021 6:12:40 PM
WebCacheV01.dat.FileSlack	12,256	File Slack	
WebCacheV01.jfm	16	Regular File	

```
y  ÎC¶$3:ywC:\Users\Administrator\AppData\Local\Microsoft\Windows\WebCache\C:\Users\Administrator\AppData\Local\Microsoft\Windows\WebCache\
```

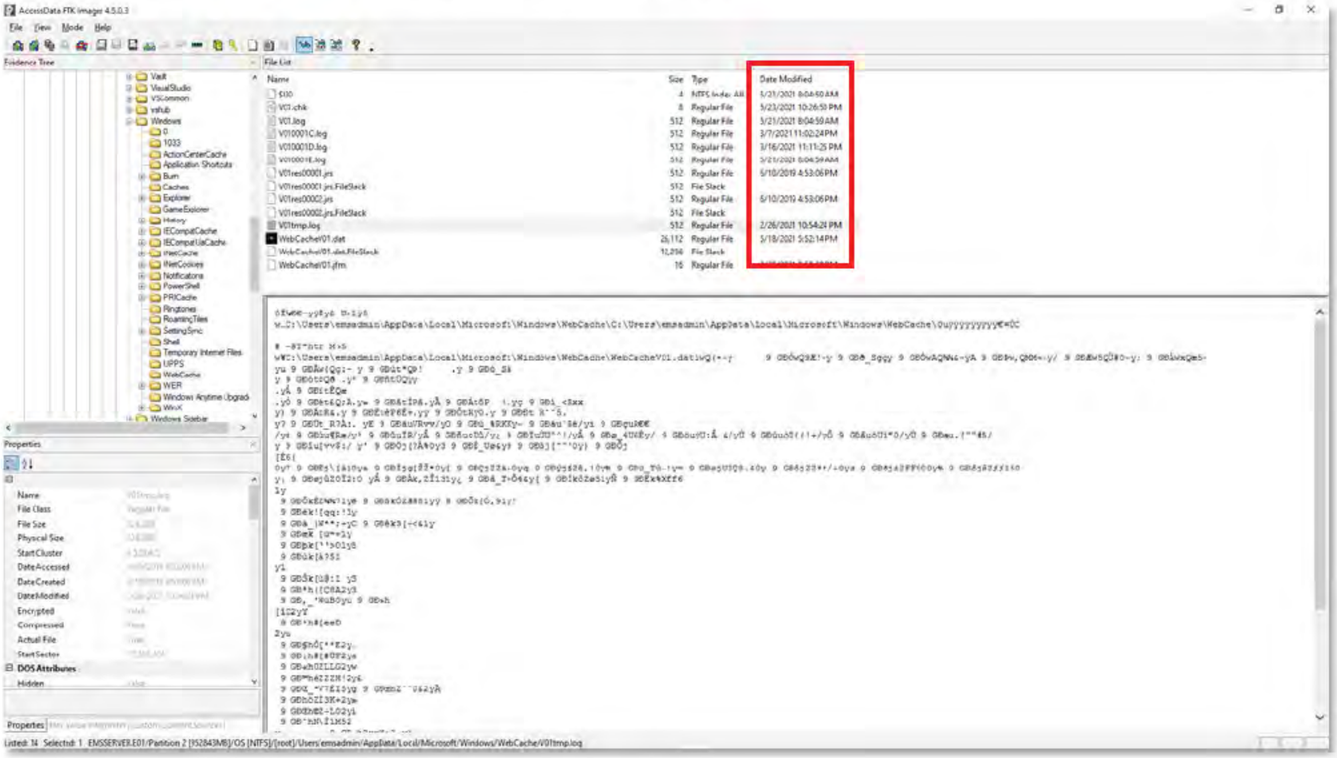
Listed: 31 Selected: 1 EMSSERVER_v2.E01/Partition 4 [952740MB]/EMS [NTFS]/[root]/Users/Administrator/AppData/Local/Microsoft/Windows/WebCache/V01tmp.log

All the Before files have been replaced with new files, replacing the originals and therefore making it impossible or nearly impossible to recover.

Server 'emsadmin' WebCache Log Files Overwritten

Purpose: *These log files store information about websites visited, files opened, etc.*

Figure 19 - EMS Server (5.11-CO) "emsadmin" WebCache Log Files Before

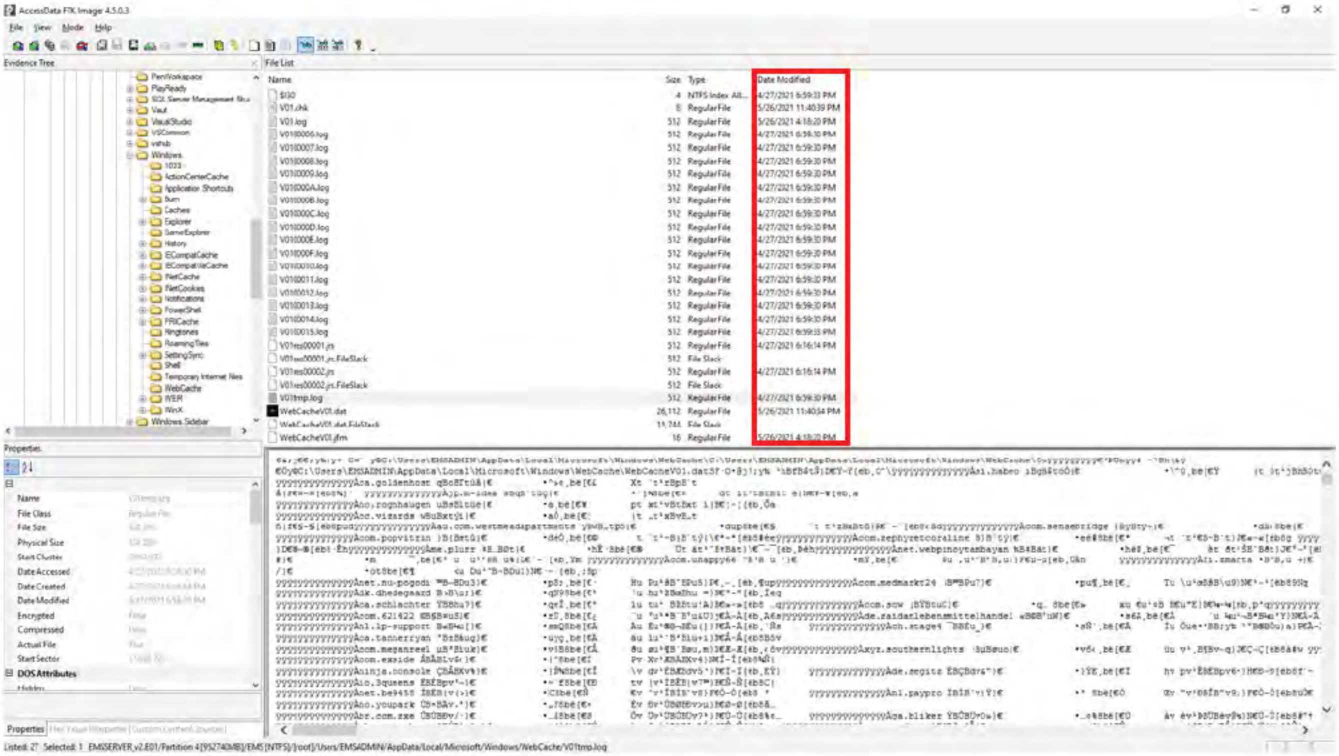


Name	Size	Type	Date Modified
$I30	4	NTFS Index All	3/21/2021 8:04:50 AM
V01.chk	8	Regular File	5/23/2021 10:26:50 PM
V01.log	512	Regular File	3/21/2021 8:04:59 AM
V010001C.log	512	Regular File	3/7/2021 11:02:24 PM
V010001D.log	512	Regular File	3/16/2021 11:11:25 PM
V010001E.log	512	Regular File	3/21/2021 8:04:59 AM
V01res00001.jrs	512	Regular File	5/10/2019 4:53:06 PM
V01res00001.jrs.FileSlack	512	File Slack	
V01res00002.jrs	512	Regular File	5/10/2019 4:53:06 PM
V01res00002.jrs.FileSlack	512	File Slack	
V01tmp.log	512	Regular File	2/26/2021 10:54:24 PM
WebCacheV01.dat	26,112	Regular File	5/18/2021 5:52:14 PM
WebCacheV01.dat.FileSlack	12,256	File Slack	
WebCacheV01.jfm	16	Regular File	[illegible]

```
w.C:\Users\emsadmin\AppData\Local\Microsoft\Windows\WebCache\C:\Users\emsadmin\AppData\Local\Microsoft\Windows\WebCache\
wWC:\Users\emsadmin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
```

Listed: 14 Selected: 1 EMSSERVER.E01/Partition 2 [152843MB]/OS [NTFS]/[root]/Users/emsadmin/AppData/Local/Microsoft/Windows/WebCache/V01tmp.log

Figure 20 -EMS Server (5.13) "emsadmin" WebCache Log Files After



Name	Size	Type	Date Modified
$I30	4	NTFS Index All...	4/27/2021 6:59:33 PM
V01.chk	8	Regular File	5/26/2021 11:40:39 PM
V01.log	512	Regular File	5/26/2021 4:18:20 PM
V0100006.log	512	Regular File	4/27/2021 6:59:30 PM
V0100007.log	512	Regular File	4/27/2021 6:59:30 PM
V0100008.log	512	Regular File	4/27/2021 6:59:30 PM
V0100009.log	512	Regular File	4/27/2021 6:59:30 PM
V010000A.log	512	Regular File	4/27/2021 6:59:30 PM
V010000B.log	512	Regular File	4/27/2021 6:59:30 PM
V010000C.log	512	Regular File	4/27/2021 6:59:30 PM
V010000D.log	512	Regular File	4/27/2021 6:59:30 PM
V010000E.log	512	Regular File	4/27/2021 6:59:30 PM
V010000F.log	512	Regular File	4/27/2021 6:59:30 PM
V0100010.log	512	Regular File	4/27/2021 6:59:30 PM
V0100011.log	512	Regular File	4/27/2021 6:59:30 PM
V0100012.log	512	Regular File	4/27/2021 6:59:30 PM
V0100013.log	512	Regular File	4/27/2021 6:59:30 PM
V0100014.log	512	Regular File	4/27/2021 6:59:30 PM
V0100015.log	512	Regular File	4/27/2021 6:59:33 PM
V01res00001.jrs	512	Regular File	4/27/2021 6:16:14 PM
V01res00001.jrs.FileSlack	512	File Slack	
V01res00002.jrs	512	Regular File	4/27/2021 6:16:14 PM
V01res00002.jrs.FileSlack	512	File Slack	
V01tmp.log	512	Regular File	4/27/2021 6:59:30 PM
WebCacheV01.dat	26,112	Regular File	5/26/2021 11:40:34 PM
WebCacheV01.dat.FileSlack	11,744	File Slack	
WebCacheV01.jfm	16	Regular File	5/26/2021 4:18:20 PM

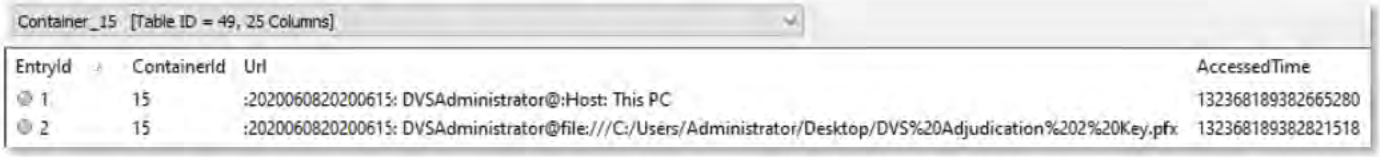
```
€ÖyC:\Users\EMSADMIN\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÅca.goldenhost
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÅjp.m-idea
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÅno.roghaugen
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÅnz.wizards
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÅau.com.westmeadapartments
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÅcom.popvitrin
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÅme.pluzz
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÅnet.nu-pogodi
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÅsk.dhedegaard
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÅca.schlachter
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÅcom.621422
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÅnl.ip-support
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÅca.tannerryan
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÅcom.meganreel
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÅcom.exside
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÅninja.console
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÅio.3queens
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÅnet.be4450
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÅno.youpark
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÅbr.com.zxe
```

Listed: 27 Selected: 1 EMSSERVER_v2.E01/Partition 4 [952740MB]/EMS [NTFS]/[root]/Users/EMSADMIN/AppData/Local/Microsoft/Windows/WebCache/V01tmp.log

The WebCache log files have been overwritten. IF the computer has been used on the Internet or with ANY webserver (even one on the local network, including this computer's OWN webserver), these WebCache files indicate the connections that were sought, as well as files that were opened. These may provide *critical* evidence that the system has been connected to a network, including networks that have access to the Internet. THESE ARE NOT the same files in the before and after images. They have been deleted and replaced.

Here is a small subset of some of the information that was found on the Before image in these WebCache log files:

Figure 21 - EMS Server (5.11-CO) Webcache Log File Content Before

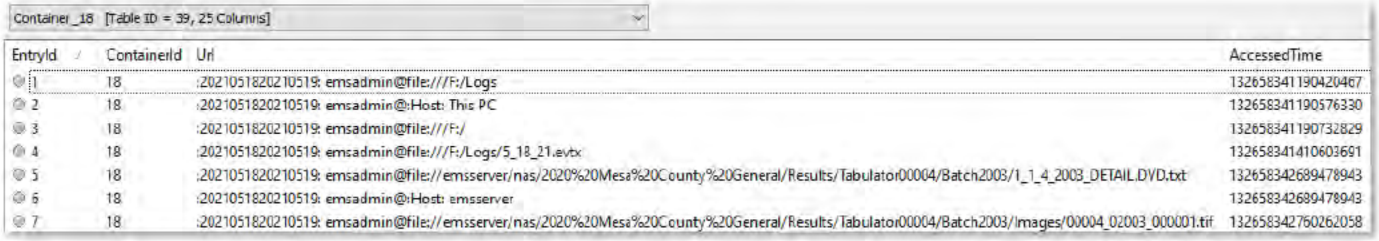


Container_15 [Table ID = 49, 25 Columns]

EntryId	ContainerId	Url	AccessedTime
1	15	:2020060820200615: DVSAdministrator@:Host: This PC	132368189382665280
2	15	:2020060820200615: DVSAdministrator@file:///C:/Users/Administrator/Desktop/DVS%20Adjudication%202%20Key.pfx	132368189382821518

For instance, the above log file entry seems to show a DVS Adjudication Encryption Key was accessed, where it was stored and accessed from, and when it was accessed.

Figure 22 - EMS SErver (5.11-CO) Webcache Log File Content Before - II



Container_18 [Table ID = 39, 25 Columns]

EntryId	ContainerId	Url	AccessedTime
1	18	:2021051820210519: emsadmin@file:///F:/Logs	132658341190420467
2	18	:2021051820210519: emsadmin@:Host: This PC	132658341190576330
3	18	:2021051820210519: emsadmin@file:///F:/	132658341190732829
4	18	:2021051820210519: emsadmin@file:///F:/Logs/5_18_21.evtx	132658341410603691
5	18	:2021051820210519: emsadmin@file://emsserver/nas/2020%20Mesa%20County%20General/Results/Tabulator00004/Batch2003/1_1_4_2003_DETAIL.DVD.txt	132658342689478943
6	18	:2021051820210519: emsadmin@:Host: emsserver	132658342689478943
7	18	:2021051820210519: emsadmin@file://emsserver/nas/2020%20Mesa%20County%20General/Results/Tabulator00004/Batch2003/Images/00004_02003_000001.tif	132658342760262058

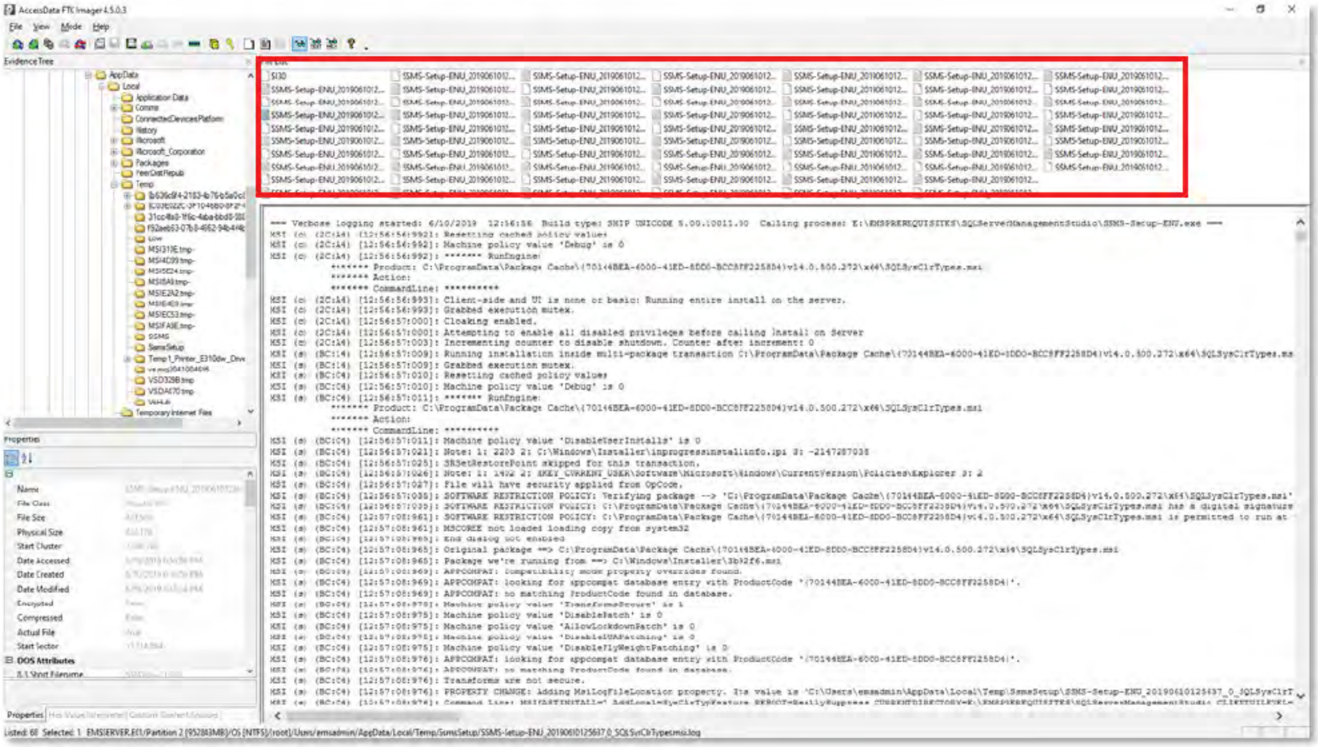
In addition, the above log file entry seems to show several interesting files (a windows 'evtx' log file being opened from an external attached USB flash drive, and a ballot detail file and even a ballot image from Batch 2003 being opened from a Network Attached Storage device)

Without a forensic Before image prior to a Dominion 'Update', this type of potentially critically-important forensic information could be, and likely would be, lost forever.

Server SQL Server Management Studio (SSMS) Log Files Overwritten

Purpose: *These log files track the installation of the SQL Server Management Studio, which is used to get into the back-end of the election databases.*

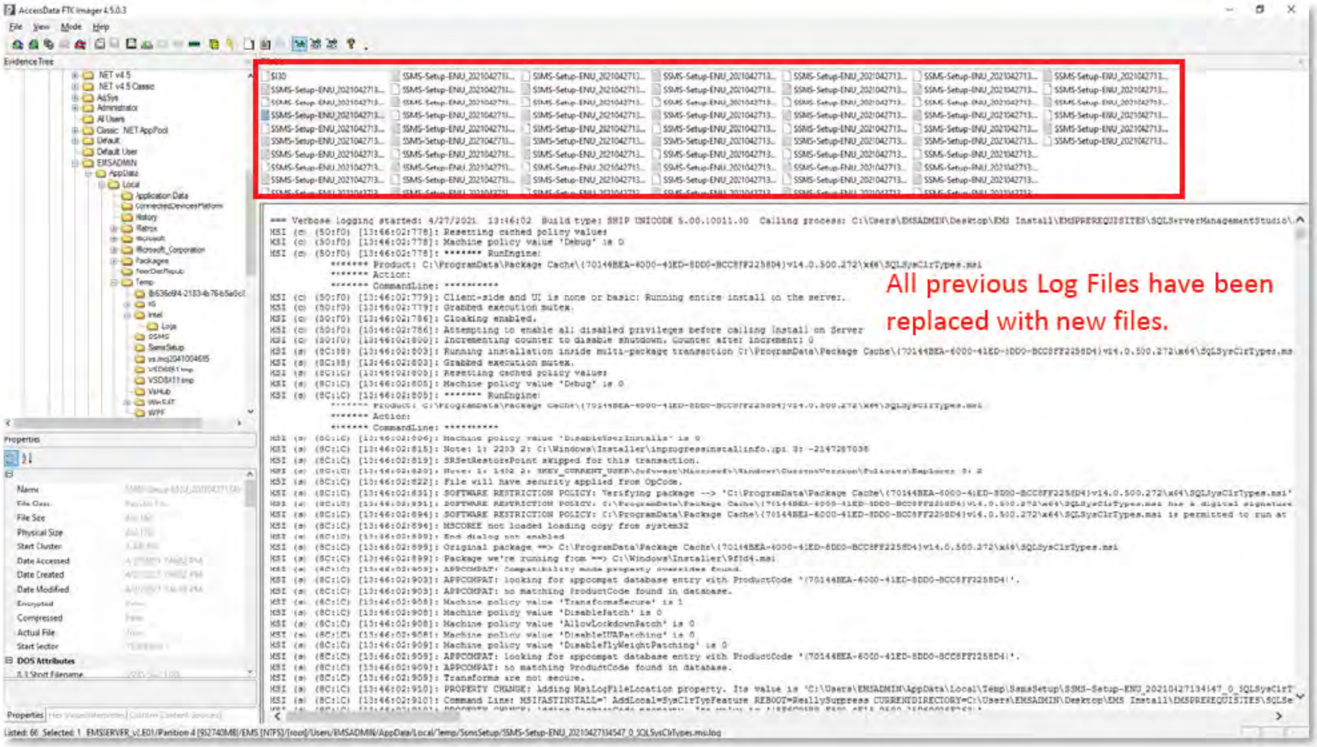
Figure 23 - EMS Server (5.11-CO) SSMS Log Files Before



```
=== Verbose logging started: 6/10/2019  12:56:56  Build type: SHIP UNICODE 5.00.10011.00  Calling process: E:\EMSPREREQUISITES\SQLServerManagementStudio\SSMS-Setup-ENU.exe ===
MSI (c) (2C:A4) [12:56:56:992]: Resetting cached policy values
MSI (c) (2C:A4) [12:56:56:992]: Machine policy value 'Debug' is 0
MSI (c) (2C:A4) [12:56:56:992]: ******* RunEngine:
           ******* Product: C:\ProgramData\Package Cache\{70144BEA-4000-41ED-8DD0-BCC8FF2258D4}v14.0.500.272\x64\SQLSysClrTypes.msi
           ******* Action:
           ******* CommandLine: **********
MSI (c) (2C:A4) [12:56:56:993]: Client-side and UI is none or basic: Running entire install on the server.
MSI (c) (2C:A4) [12:56:56:993]: Grabbed execution mutex.
MSI (c) (2C:A4) [12:56:57:000]: Cloaking enabled.
MSI (c) (2C:A4) [12:56:57:000]: Attempting to enable all disabled privileges before calling Install on Server
MSI (c) (2C:A4) [12:56:57:003]: Incrementing counter to disable shutdown. Counter after increment: 0
MSI (s) (BC:14) [12:56:57:009]: Running installation inside multi-package transaction C:\ProgramData\Package Cache\{70144BEA-4000-41ED-8DD0-BCC8FF2258D4}v14.0.500.272\x64\SQLSysClrTypes.ms
MSI (s) (BC:14) [12:56:57:009]: Grabbed execution mutex.
MSI (s) (BC:C4) [12:56:57:010]: Resetting cached policy values
MSI (s) (BC:C4) [12:56:57:010]: Machine policy value 'Debug' is 0
MSI (s) (BC:C4) [12:56:57:011]: ******* RunEngine:
           ******* Product: C:\ProgramData\Package Cache\{70144BEA-4000-41ED-8DD0-BCC8FF2258D4}v14.0.500.272\x64\SQLSysClrTypes.msi
           ******* Action:
           ******* CommandLine: **********
MSI (s) (BC:C4) [12:56:57:011]: Machine policy value 'DisableUserInstalls' is 0
MSI (s) (BC:C4) [12:56:57:021]: Note: 1: 2203 2: C:\Windows\Installer\inprogressinstallinfo.ipi 3: -2147287038
MSI (s) (BC:C4) [12:56:57:025]: SRSetRestorePoint skipped for this transaction.
MSI (s) (BC:C4) [12:56:57:026]: Note: 1: 1402 2: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 3: 2
MSI (s) (BC:C4) [12:56:57:027]: File will have security applied from OpCode.
MSI (s) (BC:C4) [12:56:57:035]: SOFTWARE RESTRICTION POLICY: Verifying package --> 'C:\ProgramData\Package Cache\{70144BEA-4000-41ED-8DD0-BCC8FF2258D4}v14.0.500.272\x64\SQLSysClrTypes.msi'
MSI (s) (BC:C4) [12:56:57:035]: SOFTWARE RESTRICTION POLICY: C:\ProgramData\Package Cache\{70144BEA-4000-41ED-8DD0-BCC8FF2258D4}v14.0.500.272\x64\SQLSysClrTypes.msi has a digital signature
MSI (s) (BC:C4) [12:57:08:961]: SOFTWARE RESTRICTION POLICY: C:\ProgramData\Package Cache\{70144BEA-4000-41ED-8DD0-BCC8FF2258D4}v14.0.500.272\x64\SQLSysClrTypes.msi is permitted to run at
MSI (s) (BC:C4) [12:57:08:961]: MSCOREE not loaded loading copy from system32
MSI (s) (BC:C4) [12:57:08:965]: End dialog not enabled
MSI (s) (BC:C4) [12:57:08:965]: Original package ==> C:\ProgramData\Package Cache\{70144BEA-4000-41ED-8DD0-BCC8FF2258D4}v14.0.500.272\x64\SQLSysClrTypes.msi
MSI (s) (BC:C4) [12:57:08:965]: Package we're running from ==> C:\Windows\Installer\3b92f6.msi
MSI (s) (BC:C4) [12:57:08:969]: APPCOMPAT: Compatibility mode property overrides found.
MSI (s) (BC:C4) [12:57:08:969]: APPCOMPAT: looking for appcompat database entry with ProductCode '{70144BEA-4000-41ED-8DD0-BCC8FF2258D4}'.
MSI (s) (BC:C4) [12:57:08:969]: APPCOMPAT: no matching ProductCode found in database.
MSI (s) (BC:C4) [12:57:08:975]: Machine policy value 'TransformsSecure' is 1
MSI (s) (BC:C4) [12:57:08:975]: Machine policy value 'DisablePatch' is 0
MSI (s) (BC:C4) [12:57:08:975]: Machine policy value 'AllowLockdownPatch' is 0
MSI (s) (BC:C4) [12:57:08:975]: Machine policy value 'DisableLUAPatching' is 0
MSI (s) (BC:C4) [12:57:08:975]: Machine policy value 'DisableFlyWeightPatching' is 0
MSI (s) (BC:C4) [12:57:08:976]: APPCOMPAT: looking for appcompat database entry with ProductCode '{70144BEA-4000-41ED-8DD0-BCC8FF2258D4}'.
MSI (s) (BC:C4) [12:57:08:976]: APPCOMPAT: no matching ProductCode found in database.
MSI (s) (BC:C4) [12:57:08:976]: Transforms are not secure.
MSI (s) (BC:C4) [12:57:08:976]: PROPERTY CHANGE: Adding MsiLogFileLocation property. Its value is 'C:\Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125437_0_SQLSysClrT
MSI (s) (BC:C4) [12:57:08:976]: Command Line: MSIFASTINSTALL=7 AddLocal=SysClrTypFeature REBOOT=ReallySuppress CURRENTDIRECTORY=E:\EMSPREREQUISITES\SQLServerManagementStudio CLIENTUILEVEL=
```

Listed: 60 Selected: 1 EMSSERVER.E01/Partition 2 [952883MB]/OS [NTFS]/[root]/Users/emsadmin/AppData/Local/Temp/SsmsSetup/SSMS-Setup-ENU_20190610125637_0_SQLSysClrTypes.msi.log

Figure 24 - EMS Server (5.13) SSMS Log Files After



```
=== Verbose logging started: 4/27/2021  13:46:02  Build type: SHIP UNICODE 5.00.10011.00  Calling process: C:\Users\EMSADMIN\Desktop\EMS Install\EMSPREREQUISITES\SQLServerManagementStudio\
MSI (c) (50:F0) [13:46:02:778]: Resetting cached policy values
MSI (c) (50:F0) [13:46:02:778]: Machine policy value 'Debug' is 0
MSI (c) (50:F0) [13:46:02:778]: ******* RunEngine:
           ******* Product: C:\ProgramData\Package Cache\{70144BEA-4000-41ED-8DD0-BCC8FF2258D4}v14.0.500.272\x64\SQLSysClrTypes.msi
           ******* Action:
           ******* CommandLine: **********
MSI (c) (50:F0) [13:46:02:779]: Client-side and UI is none or basic: Running entire install on the server.
MSI (c) (50:F0) [13:46:02:779]: Grabbed execution mutex.
MSI (c) (50:F0) [13:46:02:786]: Cloaking enabled.
MSI (c) (50:F0) [13:46:02:786]: Attempting to enable all disabled privileges before calling Install on Server
MSI (c) (50:F0) [13:46:02:800]: Incrementing counter to disable shutdown. Counter after increment: 0
MSI (s) (8C:38) [13:46:02:803]: Running installation inside multi-package transaction C:\ProgramData\Package Cache\{70144BEA-4000-41ED-8DD0-BCC8FF2258D4}v14.0.500.272\x64\SQLSysClrTypes.ms
MSI (s) (8C:38) [13:46:02:803]: Grabbed execution mutex.
MSI (s) (8C:1C) [13:46:02:805]: Resetting cached policy values
MSI (s) (8C:1C) [13:46:02:805]: Machine policy value 'Debug' is 0
MSI (s) (8C:1C) [13:46:02:805]: ******* RunEngine:
           ******* Product: C:\ProgramData\Package Cache\{70144BEA-4000-41ED-8DD0-BCC8FF2258D4}v14.0.500.272\x64\SQLSysClrTypes.msi
           ******* Action:
           ******* CommandLine: **********
MSI (s) (8C:1C) [13:46:02:806]: Machine policy value 'DisableUserInstalls' is 0
MSI (s) (8C:1C) [13:46:02:815]: Note: 1: 2203 2: C:\Windows\Installer\inprogressinstallinfo.ipi 3: -2147287038
MSI (s) (8C:1C) [13:46:02:819]: SRSetRestorePoint skipped for this transaction.
MSI (s) (8C:1C) [13:46:02:820]: Note: 1: 1402 2: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 3: 2
MSI (s) (8C:1C) [13:46:02:822]: File will have security applied from OpCode.
MSI (s) (8C:1C) [13:46:02:831]: SOFTWARE RESTRICTION POLICY: Verifying package --> 'C:\ProgramData\Package Cache\{70144BEA-4000-41ED-8DD0-BCC8FF2258D4}v14.0.500.272\x64\SQLSysClrTypes.msi'
MSI (s) (8C:1C) [13:46:02:831]: SOFTWARE RESTRICTION POLICY: C:\ProgramData\Package Cache\{70144BEA-4000-41ED-8DD0-BCC8FF2258D4}v14.0.500.272\x64\SQLSysClrTypes.msi has a digital signature
MSI (s) (8C:1C) [13:46:02:894]: SOFTWARE RESTRICTION POLICY: C:\ProgramData\Package Cache\{70144BEA-4000-41ED-8DD0-BCC8FF2258D4}v14.0.500.272\x64\SQLSysClrTypes.msi is permitted to run at
MSI (s) (8C:1C) [13:46:02:894]: MSCOREE not loaded loading copy from system32
MSI (s) (8C:1C) [13:46:02:899]: End dialog not enabled
MSI (s) (8C:1C) [13:46:02:899]: Original package ==> C:\ProgramData\Package Cache\{70144BEA-4000-41ED-8DD0-BCC8FF2258D4}v14.0.500.272\x64\SQLSysClrTypes.msi
MSI (s) (8C:1C) [13:46:02:899]: Package we're running from ==> C:\Windows\Installer\9f8d4.msi
MSI (s) (8C:1C) [13:46:02:903]: APPCOMPAT: Compatibility mode property overrides found.
MSI (s) (8C:1C) [13:46:02:903]: APPCOMPAT: looking for appcompat database entry with ProductCode '{70144BEA-4000-41ED-8DD0-BCC8FF2258D4}'.
MSI (s) (8C:1C) [13:46:02:903]: APPCOMPAT: no matching ProductCode found in database.
MSI (s) (8C:1C) [13:46:02:908]: Machine policy value 'TransformsSecure' is 1
MSI (s) (8C:1C) [13:46:02:908]: Machine policy value 'DisablePatch' is 0
MSI (s) (8C:1C) [13:46:02:908]: Machine policy value 'AllowLockdownPatch' is 0
MSI (s) (8C:1C) [13:46:02:908]: Machine policy value 'DisableLUAPatching' is 0
MSI (s) (8C:1C) [13:46:02:909]: Machine policy value 'DisableFlyWeightPatching' is 0
MSI (s) (8C:1C) [13:46:02:909]: APPCOMPAT: looking for appcompat database entry with ProductCode '{70144BEA-4000-41ED-8DD0-BCC8FF2258D4}'.
MSI (s) (8C:1C) [13:46:02:909]: APPCOMPAT: no matching ProductCode found in database.
MSI (s) (8C:1C) [13:46:02:909]: Transforms are not secure.
MSI (s) (8C:1C) [13:46:02:910]: PROPERTY CHANGE: Adding MsiLogFileLocation property. Its value is 'C:\Users\EMSADMIN\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20210427134147_0_SQLSysClrT
MSI (s) (8C:1C) [13:46:02:910]: Command Line: MSIFASTINSTALL=7 AddLocal=SysClrTypFeature REBOOT=ReallySuppress CURRENTDIRECTORY=C:\Users\EMSADMIN\Desktop\EMS Install\EMSPREREQUISITES\SQLSe
```

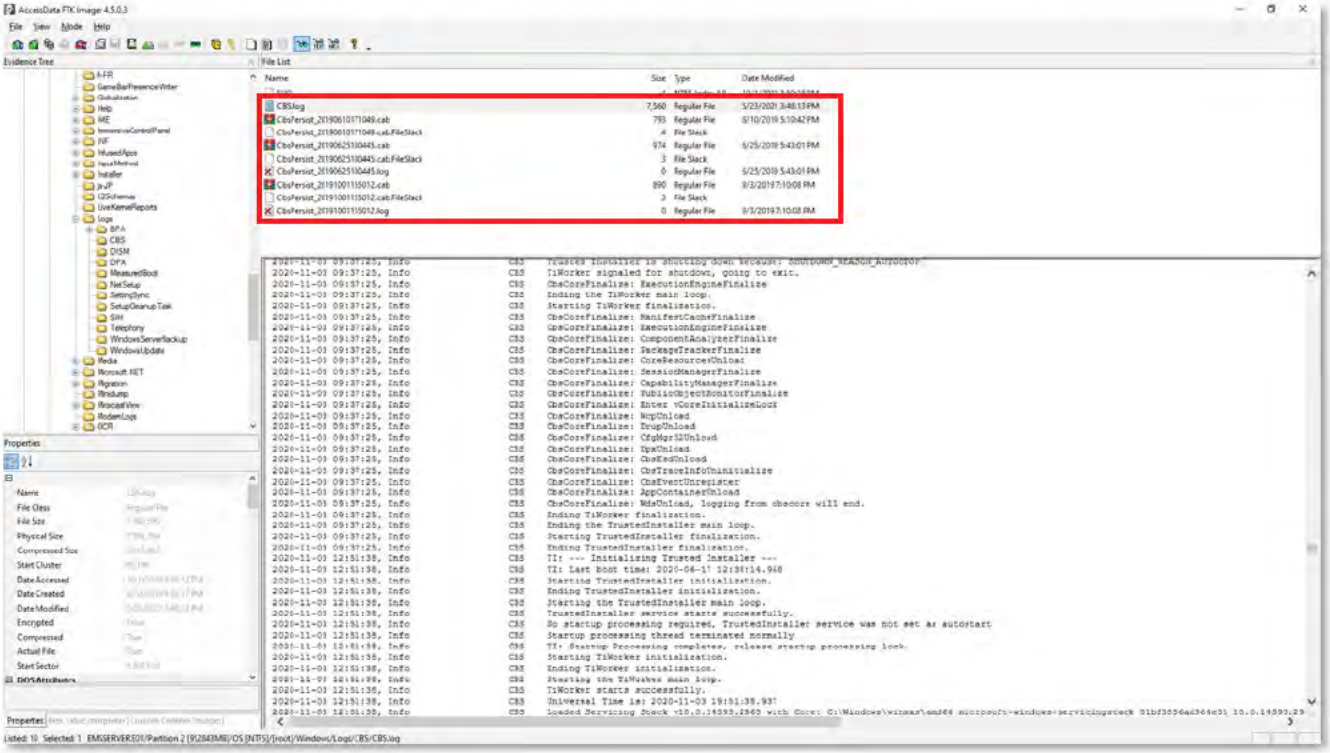
All previous Log Files have been replaced with new files.

Listed: 66 Selected: 1 EMSSERVER_v1.E01/Partition 4 [952740MB]/EMS [NTFS]/[root]/Users/EMSADMIN/AppData/Local/Temp/SsmsSetup/SSMS-Setup-ENU_20210427134547_0_SQLSysClrTypes.msi.log

Server CBS Log Files Overwritten

Purpose: *These Log Files contain detailed information about installed updates. They could contain evidence of changes to the server that would cause decertification of the system.*

Figure 25 - EMS Server (5.11-CO) CBS Log Files Before

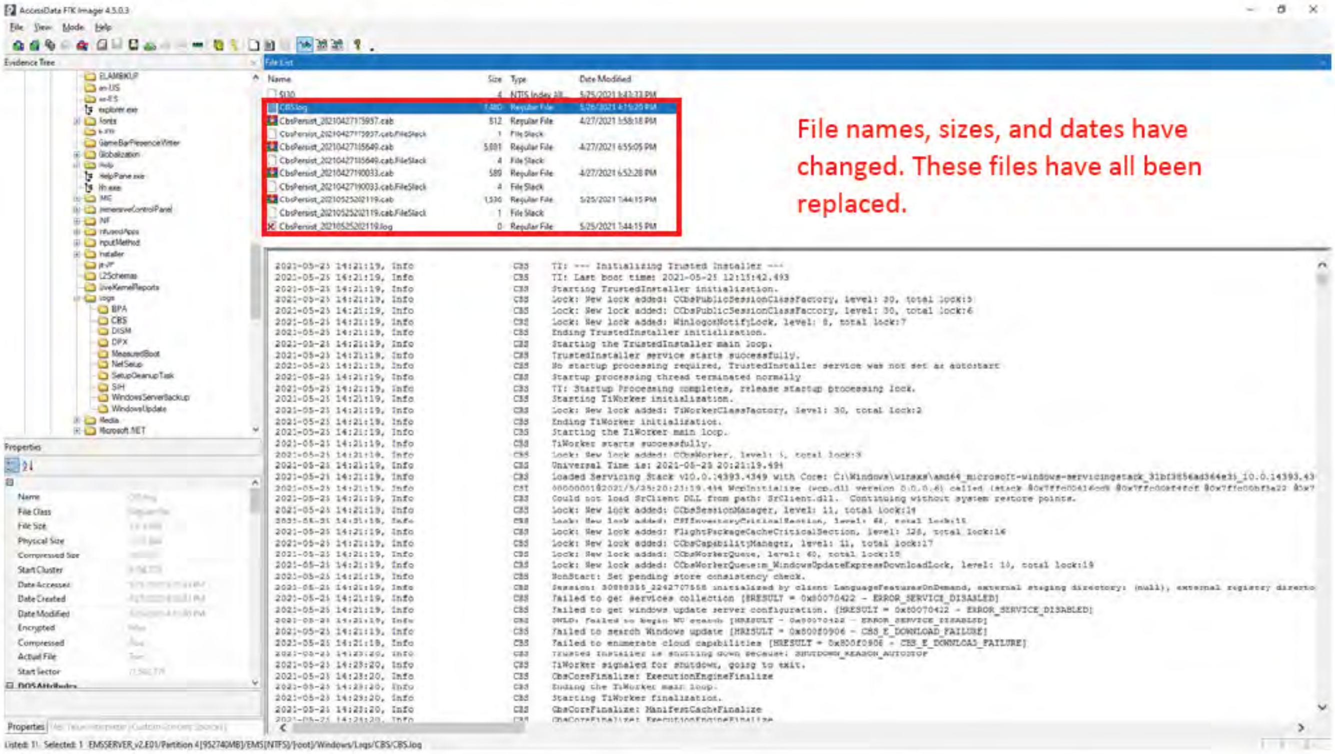


Name	Size	Type	Date Modified
CBS.log	7,560	Regular File	5/23/2021 3:48:13 PM
CbsPersist_20190610171049.cab	793	Regular File	6/10/2019 5:10:42 PM
CbsPersist_20190610171049.cab.FileSlack	4	File Slack	
CbsPersist_20190625110445.cab	974	Regular File	6/25/2019 5:43:01 PM
CbsPersist_20190625110445.cab.FileSlack	3	File Slack	
CbsPersist_20190625110445.log	0	Regular File	6/25/2019 5:43:01 PM
CbsPersist_20191001115012.cab	890	Regular File	9/3/2019 7:10:08 PM
CbsPersist_20191001115012.cab.FileSlack	3	File Slack	
CbsPersist_20191001115012.log	0	Regular File	9/3/2019 7:10:08 PM

```
2020-11-03 09:37:25, Info                  CBS    Trusted Installer is shutting down because: SHUTDOWN_REASON_AUTOSTOP
2020-11-03 09:37:25, Info                  CBS    TiWorker signaled for shutdown, going to exit.
2020-11-03 09:37:25, Info                  CBS    CbsCoreFinalize: ExecutionEngineFinalize
2020-11-03 09:37:25, Info                  CBS    Ending the TiWorker main loop.
2020-11-03 09:37:25, Info                  CBS    Starting TiWorker finalization.
2020-11-03 09:37:25, Info                  CBS    CbsCoreFinalize: ManifestCacheFinalize
2020-11-03 09:37:25, Info                  CBS    CbsCoreFinalize: ExecutionEngineFinalize
2020-11-03 09:37:25, Info                  CBS    CbsCoreFinalize: ComponentAnalyzerFinalize
2020-11-03 09:37:25, Info                  CBS    CbsCoreFinalize: PackageTrackerFinalize
2020-11-03 09:37:25, Info                  CBS    CbsCoreFinalize: CoreResourcesUnload
2020-11-03 09:37:25, Info                  CBS    CbsCoreFinalize: SessionManagerFinalize
2020-11-03 09:37:25, Info                  CBS    CbsCoreFinalize: CapabilityManagerFinalize
2020-11-03 09:37:25, Info                  CBS    CbsCoreFinalize: PublicObjectMonitorFinalize
2020-11-03 09:37:25, Info                  CBS    CbsCoreFinalize: Enter vCoreInitializeLock
2020-11-03 09:37:25, Info                  CBS    CbsCoreFinalize: WcpUnload
2020-11-03 09:37:25, Info                  CBS    CbsCoreFinalize: DrupUnload
2020-11-03 09:37:25, Info                  CBS    CbsCoreFinalize: CfgMgr32Unload
2020-11-03 09:37:25, Info                  CBS    CbsCoreFinalize: DpxUnload
2020-11-03 09:37:25, Info                  CBS    CbsCoreFinalize: CbsEsdUnload
2020-11-03 09:37:25, Info                  CBS    CbsCoreFinalize: CbsTraceInfoUninitialize
2020-11-03 09:37:25, Info                  CBS    CbsCoreFinalize: CbsEventUnregister
2020-11-03 09:37:25, Info                  CBS    CbsCoreFinalize: AppContainerUnload
2020-11-03 09:37:25, Info                  CBS    CbsCoreFinalize: WdsUnload, logging from cbscore will end.
2020-11-03 09:37:25, Info                  CBS    Ending TiWorker finalization.
2020-11-03 09:37:25, Info                  CBS    Ending the TrustedInstaller main loop.
2020-11-03 09:37:25, Info                  CBS    Starting TrustedInstaller finalization.
2020-11-03 09:37:25, Info                  CBS    Ending TrustedInstaller finalization.
2020-11-03 12:51:38, Info                  CBS    TI: --- Initializing Trusted Installer ---
2020-11-03 12:51:38, Info                  CBS    TI: Last boot time: 2020-06-17 12:38:14.948
2020-11-03 12:51:38, Info                  CBS    Starting TrustedInstaller initialization.
2020-11-03 12:51:38, Info                  CBS    Ending TrustedInstaller initialization.
2020-11-03 12:51:38, Info                  CBS    Starting the TrustedInstaller main loop.
2020-11-03 12:51:38, Info                  CBS    TrustedInstaller service starts successfully.
2020-11-03 12:51:38, Info                  CBS    No startup processing required, TrustedInstaller service was not set as autostart
2020-11-03 12:51:38, Info                  CBS    Startup processing thread terminated normally
2020-11-03 12:51:38, Info                  CBS    TI: Startup Processing completes, release startup processing lock.
2020-11-03 12:51:38, Info                  CBS    Starting TiWorker initialization.
2020-11-03 12:51:38, Info                  CBS    Ending TiWorker initialization.
2020-11-03 12:51:38, Info                  CBS    Starting the TiWorker main loop.
2020-11-03 12:51:38, Info                  CBS    TiWorker starts successfully.
2020-11-03 12:51:38, Info                  CBS    Universal Time is: 2020-11-03 19:51:38.937
2020-11-03 12:51:38, Info                  CBS    Loaded Servicing Stack v10.0.14393.2363 with Core: C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.14393.29
```

Listed: 10 Selected: 1 EMSSERVER01/Partition 2 [912843MB]/OS [NTFS]/[root]/Windows/Logs/CBS/CBS.log

Figure 26 - EMS Server (5.13) CBS Log Files After



Name	Size	Type	Date Modified
$I30	4	NTFS Index All...	5/25/2021 3:43:33 PM
CBS.log	7,480	Regular File	5/26/2021 4:15:20 PM
CbsPersist_20210427115937.cab	512	Regular File	4/27/2021 3:58:18 PM
CbsPersist_20210427115937.cab.FileSlack	1	File Slack	
CbsPersist_20210427115649.cab	5,001	Regular File	4/27/2021 6:55:05 PM
CbsPersist_20210427115649.cab.FileSlack	4	File Slack	
CbsPersist_20210427190033.cab	589	Regular File	4/27/2021 6:52:28 PM
CbsPersist_20210427190033.cab.FileSlack	4	File Slack	
CbsPersist_20210525202119.cab	1,536	Regular File	5/25/2021 1:44:15 PM
CbsPersist_20210525202119.cab.FileSlack	1	File Slack	
CbsPersist_20210525202119.log	0	Regular File	5/25/2021 1:44:15 PM

```
2021-05-25 14:21:19, Info                  CBS    TI: --- Initializing Trusted Installer ---
2021-05-25 14:21:19, Info                  CBS    TI: Last boot time: 2021-05-25 12:15:42.493
2021-05-25 14:21:19, Info                  CBS    Starting TrustedInstaller initialization.
2021-05-25 14:21:19, Info                  CBS    Lock: New lock added: CCbsPublicSessionClassFactory, level: 30, total lock:5
2021-05-25 14:21:19, Info                  CBS    Lock: New lock added: CCbsPublicSessionClassFactory, level: 30, total lock:6
2021-05-25 14:21:19, Info                  CBS    Lock: New lock added: WinlogonNotifyLock, level: 8, total lock:7
2021-05-25 14:21:19, Info                  CBS    Ending TrustedInstaller initialization.
2021-05-25 14:21:19, Info                  CBS    Starting the TrustedInstaller main loop.
2021-05-25 14:21:19, Info                  CBS    TrustedInstaller service starts successfully.
2021-05-25 14:21:19, Info                  CBS    No startup processing required, TrustedInstaller service was not set as autostart
2021-05-25 14:21:19, Info                  CBS    Startup processing thread terminated normally
2021-05-25 14:21:19, Info                  CBS    TI: Startup Processing completes, release startup processing lock.
2021-05-25 14:21:19, Info                  CBS    Starting TiWorker initialization.
2021-05-25 14:21:19, Info                  CBS    Lock: New lock added: TiWorkerClassFactory, level: 30, total lock:2
2021-05-25 14:21:19, Info                  CBS    Ending TiWorker initialization.
2021-05-25 14:21:19, Info                  CBS    Starting the TiWorker main loop.
2021-05-25 14:21:19, Info                  CBS    TiWorker starts successfully.
2021-05-25 14:21:19, Info                  CBS    Lock: New lock added: CCbsWorker, level: 5, total lock:3
2021-05-25 14:21:19, Info                  CBS    Universal Time is: 2021-05-25 20:21:19.494
2021-05-25 14:21:19, Info                  CBS    Loaded Servicing Stack v10.0.14393.4349 with Core: C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.14393.43
2021-05-25 14:21:19, Info                  CSI    00000001@2021/5/25:20:21:19.494 WcpInitialize (wcp.dll version 0.0.0.6) called (stack @0x7ffc0041... @0x7ffc00af4fcf @0x7ffc00bf3a22 @0x7
2021-05-25 14:21:19, Info                  CBS    Could not load SrClient DLL from path: SrClient.dll.  Continuing without system restore points.
2021-05-25 14:21:19, Info                  CBS    Lock: New lock added: CCbsSessionManager, level: 11, total lock:14
2021-05-25 14:21:19, Info                  CBS    Lock: New lock added: CSIInventoryCriticalSection, level: 64, total lock:15
2021-05-25 14:21:19, Info                  CBS    Lock: New lock added: FlightPackageCacheCriticalSection, level: 128, total lock:16
2021-05-25 14:21:19, Info                  CBS    Lock: New lock added: CCbsCapabilityManager, level: 11, total lock:17
2021-05-25 14:21:19, Info                  CBS    Lock: New lock added: CCbsWorkerQueue, level: 40, total lock:18
2021-05-25 14:21:19, Info                  CBS    Lock: New lock added: CCbsWorkerQueue:m_WindowsUpdateExpressDownloadLock, level: 10, total lock:19
2021-05-25 14:21:19, Info                  CBS    NonStart: Set pending store consistency check.
2021-05-25 14:21:19, Info                  CBS    Session: 30888355_2242707558 initialized by client LanguageFeaturesOnDemand, external staging directory: (null), external registry directo
2021-05-25 14:21:19, Info                  CBS    Failed to get services collection [HRESULT = 0x80070422 - ERROR_SERVICE_DISABLED]
2021-05-25 14:21:19, Info                  CBS    Failed to get windows update server configuration. [HRESULT = 0x80070422 - ERROR_SERVICE_DISABLED]
2021-05-25 14:21:19, Info                  CBS    DWLD: Failed to begin WU search [HRESULT = 0x80070422 - ERROR_SERVICE_DISABLED]
2021-05-25 14:21:19, Info                  CBS    Failed to search Windows update [HRESULT = 0x800f0906 - CBS_E_DOWNLOAD_FAILURE]
2021-05-25 14:21:19, Info                  CBS    Failed to enumerate cloud capabilities [HRESULT = 0x800f0906 - CBS_E_DOWNLOAD_FAILURE]
2021-05-25 14:23:20, Info                  CBS    Trusted Installer is shutting down because: SHUTDOWN_REASON_AUTOSTOP
2021-05-25 14:23:20, Info                  CBS    TiWorker signaled for shutdown, going to exit.
2021-05-25 14:23:20, Info                  CBS    CbsCoreFinalize: ExecutionEngineFinalize
2021-05-25 14:23:20, Info                  CBS    Ending the TiWorker main loop.
2021-05-25 14:23:20, Info                  CBS    Starting TiWorker finalization.
2021-05-25 14:23:20, Info                  CBS    CbsCoreFinalize: ManifestCacheFinalize
2021-05-25 14:23:20, Info                  CBS    CbsCoreFinalize: ExecutionEngineFinalize
```

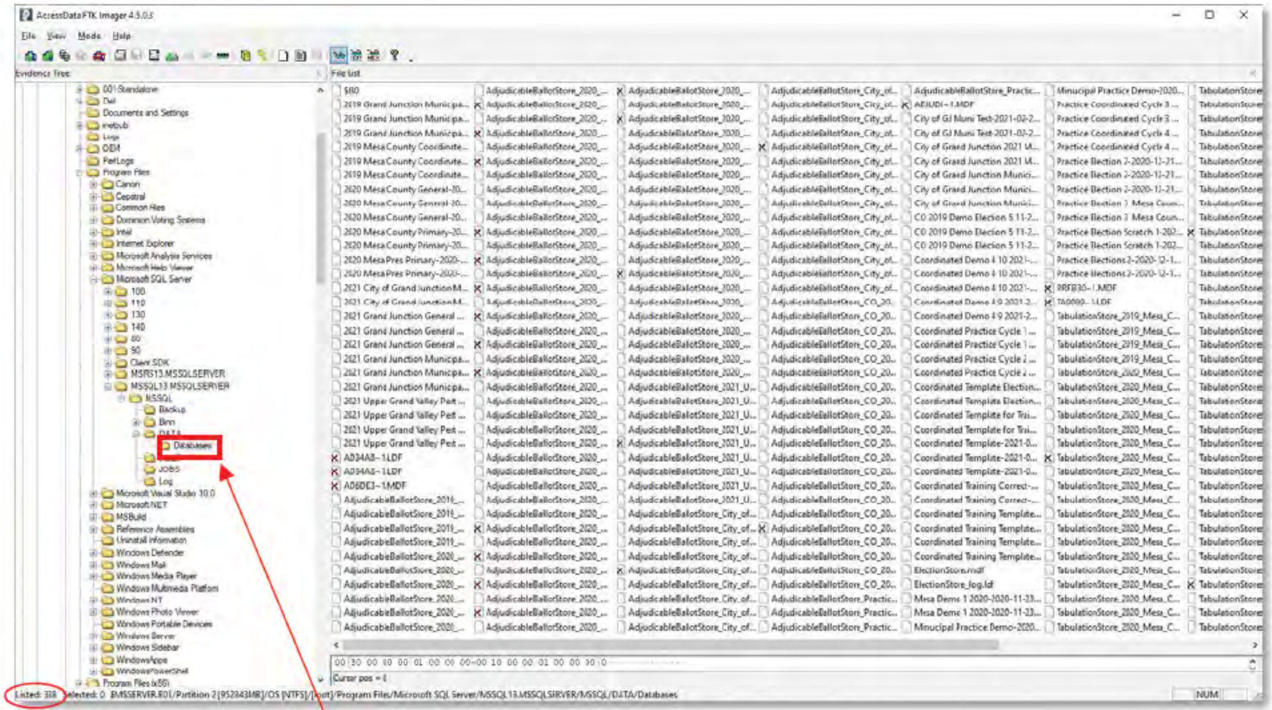
Listed: 11 Selected: 1 EMSSERVER_v2.E01/Partition 4 [952740MB]/EMS [NTFS]/[root]/Windows/Logs/CBS/CBS.log

File names, sizes, and dates have changed. These files have all been replaced.

Server Election Databases Missing

Purpose: *This folder holds all the databases (votes, information regarding batches, when they were processed, how many were processed, who they were processed by, and much more). There are also multiple extra databases that contain information regarding ballot adjudication.*

Figure 27 - EMS Server (5.11-CO) Election Databases Before

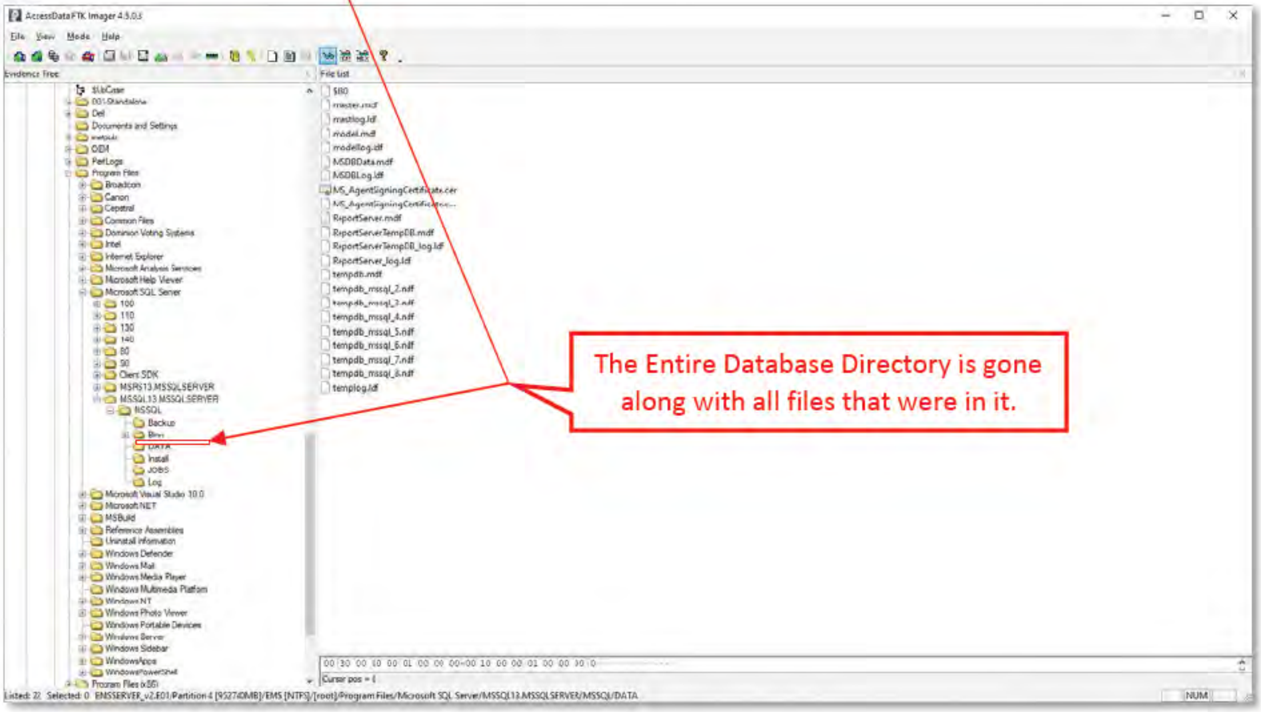


```
001 Standalone
Dell
Documents and Settings
inetpub
Logs
ODM
PerfLogs
Program Files
  Canon
  Cepstral
  Common Files
  Dominion Voting Systems
  Intel
  Internet Explorer
  Microsoft Analysis Services
  Microsoft Help Viewer
  Microsoft SQL Server
    100
    110
    130
    140
    80
    90
    Client SDK
    MSRS13.MSSQLSERVER
    MSSQL13.MSSQLSERVER
      MSSQL
        Backup
        Binn
        DATA
          Databases
        JOBS
        Log
  Microsoft Visual Studio 10.0
  Microsoft.NET
  MSBuild
  Reference Assemblies
  Uninstall Information
  Windows Defender
  Windows Mail
  Windows Media Player
  Windows Multimedia Platform
  Windows NT
  Windows Photo Viewer
  Windows Portable Devices
  Windows Server
  Windows Sidebar
  WindowsApps
  WindowsPowerShell
Program Files (x86)
```

$I80	AdjudicableBallotStore_2020_...	☒ AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	AdjudicableBallotStore_Practic...	Minucipal Practice Demo-2020...	TabulationStore
2019 Grand Junction Municipa...	☒ AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	☒ ADJUDI~1.MDF	Practice Coordinated Cycle 3 ...	TabulationStore
2019 Grand Junction Municipa...	AdjudicableBallotStore_2020_...	☒ AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	City of GJ Muni Test-2021-02-2...	Practice Coordinated Cycle 3 ...	TabulationStore
2019 Grand Junction Municipa...	☒ AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	City of GJ Muni Test-2021-02-2...	Practice Coordinated Cycle 4 ...	TabulationStore
2019 Mesa County Coordinate...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2020_...	☒ AdjudicableBallotStore_City_of...	City of Grand Junction 2021 M...	Practice Coordinated Cycle 4 ...	TabulationStore
2019 Mesa County Coordinate...	☒ AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	City of Grand Junction 2021 M...	Practice Election 2-2020-12-21...	TabulationStore
2019 Mesa County Coordinate...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	City of Grand Junction Munici...	Practice Election 2-2020-12-21...	TabulationStore
2020 Mesa County General-20...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	City of Grand Junction Munici...	Practice Election 2-2020-12-21...	TabulationStore
2020 Mesa County General-20...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	City of Grand Junction Munici...	Practice Election 3 Mesa Coun...	TabulationStore
2020 Mesa County General-20...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	CO 2019 Demo Election 5 11-2...	Practice Election 3 Mesa Coun...	TabulationStore
2020 Mesa County Primary-20...	☒ AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	CO 2019 Demo Election 5 11-2...	Practice Election Scratch 1-202...	☒ TabulationStore
2020 Mesa County Primary-20...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	CO 2019 Demo Election 5 11-2...	Practice Election Scratch 1-202...	TabulationStore
2020 Mesa Pres Primary-2020-...	☒ AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	Coordinated Demo 4 10 2021-...	Practice Elections 2-2020-12-1...	TabulationStore
2020 Mesa Pres Primary-2020-...	AdjudicableBallotStore_2020_...	☒ AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	Coordinated Demo 4 10 2021-...	Practice Elections 2-2020-12-1...	TabulationStore
2021 City of Grand Junction M...	☒ AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	Coordinated Demo 4 10 2021-...	☒ PRFB30~1.MDF	TabulationStore
2021 City of Grand Junction M...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_CO_20...	Coordinated Demo 4 9 2021-2...	☒ TA0090~1.LDF	TabulationStore
2021 Grand Junction General ...	☒ AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_CO_20...	Coordinated Demo 4 9 2021-2...	TabulationStore_2019_Mesa_C...	TabulationStore
2021 Grand Junction General ...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_CO_20...	Coordinated Practice Cycle 1 ...	TabulationStore_2019_Mesa_C...	TabulationStore
2021 Grand Junction General ...	☒ AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_CO_20...	Coordinated Practice Cycle 1 ...	TabulationStore_2019_Mesa_C...	TabulationStore
2021 Grand Junction Municipa...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_CO_20...	Coordinated Practice Cycle 2 ...	TabulationStore_2020_Mesa_C...	TabulationStore
2021 Grand Junction Municipa...	☒ AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_CO_20...	Coordinated Practice Cycle 2 ...	TabulationStore_2020_Mesa_C...	TabulationStore
2021 Grand Junction Municipa...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2021_U...	AdjudicableBallotStore_CO_20...	Coordinated Template Election...	TabulationStore_2020_Mesa_C...	TabulationStore
2021 Upper Grand Valley Pest ...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2021_U...	AdjudicableBallotStore_CO_20...	Coordinated Template Election...	TabulationStore_2020_Mesa_C...	TabulationStore
2021 Upper Grand Valley Pest ...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2021_U...	AdjudicableBallotStore_CO_20...	Coordinated Template for Trai...	TabulationStore_2020_Mesa_C...	TabulationStore
2021 Upper Grand Valley Pest ...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2021_U...	AdjudicableBallotStore_CO_20...	Coordinated Template for Trai...	TabulationStore_2020_Mesa_C...	TabulationStore
2021 Upper Grand Valley Pest ...	AdjudicableBallotStore_2020_...	☒ AdjudicableBallotStore_2021_U...	AdjudicableBallotStore_CO_20...	Coordinated Template-2021-0...	TabulationStore_2020_Mesa_C...	TabulationStore
☒ AD34A8~1LDF	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2021_U...	AdjudicableBallotStore_CO_20...	Coordinated Template-2021-0...	☒ TabulationStore_2020_Mesa_C...	TabulationStore
☒ AD34A8~1LDF	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2021_U...	AdjudicableBallotStore_CO_20...	Coordinated Template-2021-0...	TabulationStore_2020_Mesa_C...	TabulationStore
☒ AD6DE3~1.MDF	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2021_U...	AdjudicableBallotStore_CO_20...	Coordinated Training Correct-...	TabulationStore_2020_Mesa_C...	TabulationStore
AdjudicableBallotStore_2019_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2021_U...	AdjudicableBallotStore_CO_20...	Coordinated Training Correct-...	TabulationStore_2020_Mesa_C...	TabulationStore
AdjudicableBallotStore_2019_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	AdjudicableBallotStore_CO_20...	Coordinated Training Template...	TabulationStore_2020_Mesa_C...	TabulationStore
AdjudicableBallotStore_2019_...	☒ AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	☒ AdjudicableBallotStore_CO_20...	Coordinated Training Template...	TabulationStore_2020_Mesa_C...	TabulationStore
AdjudicableBallotStore_2019_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	AdjudicableBallotStore_CO_20...	Coordinated Training Template...	TabulationStore_2020_Mesa_C...	TabulationStore
AdjudicableBallotStore_2020_...	☒ AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	AdjudicableBallotStore_CO_20...	Coordinated Training Template...	TabulationStore_2020_Mesa_C...	TabulationStore
AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2020_...	☒ AdjudicableBallotStore_City_of...	AdjudicableBallotStore_CO_20...	ElectionStore.mdf	TabulationStore_2020_Mesa_C...	TabulationStore
AdjudicableBallotStore_2020_...	☒ AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	AdjudicableBallotStore_CO_20...	ElectionStore_log.ldf	TabulationStore_2020_Mesa_C...	☒ TabulationStore
AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	AdjudicableBallotStore_Practic...	Mesa Demo 1 2020-2020-11-23...	TabulationStore_2020_Mesa_C...	TabulationStore
AdjudicableBallotStore_2020_...	☒ AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	AdjudicableBallotStore_Practic...	Mesa Demo 1 2020-2020-11-23...	TabulationStore_2020_Mesa_C...	TabulationStore
AdjudicableBallotStore_2020_...	AdjudicableBallotStore_2020_...	AdjudicableBallotStore_City_of...	AdjudicableBallotStore_Practic...	Minucipal Practice Demo-2020...	TabulationStore_2020_Mesa_C...	TabulationStore

```
00 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 30 0
Cursor pos = 0
Listed: 338  Selected: 0  EMSSERVER.E01/Partition 2 [952843MB]/OS [NTFS]/[root]/Program Files/Microsoft SQL Server/MSSQL13.MSSQLSERVER/MSSQL/DATA/Databases    NUM
```

Figure 28 - EMS Server (5.13) Election Databases After



```
SubCase
001 Standalone
Dell
Documents and Settings
inetpub
ODM
PerfLogs
Program Files
  Broadcom
  Canon
  Cepstral
  Common Files
  Dominion Voting Systems
  Intel
  Internet Explorer
  Microsoft Analysis Services
  Microsoft Help Viewer
  Microsoft SQL Server
    100
    110
    130
    140
    80
    90
    Client SDK
    MSRS13.MSSQLSERVER
    MSSQL13.MSSQLSERVER
      MSSQL
        Backup
        Binn
        DATA
        Install
        JOBS
        Log
  Microsoft Visual Studio 10.0
  Microsoft.NET
  MSBuild
  Reference Assemblies
  Uninstall Information
  Windows Defender
  Windows Mail
  Windows Media Player
  Windows Multimedia Platform
  Windows NT
  Windows Photo Viewer
  Windows Portable Devices
  Windows Server
  Windows Sidebar
  WindowsApps
  WindowsPowerShell
Program Files (x86)
```

```
$I80
master.mdf
mastlog.ldf
model.mdf
modellog.ldf
MSDBData.mdf
MSDBLog.ldf
MS_AgentSigningCertificate.cer
MS_AgentSigningCertificate...
ReportServer.mdf
ReportServerTempDB.mdf
ReportServerTempDB_log.ldf
ReportServer_log.ldf
tempdb.mdf
tempdb_mssql_2.ndf
tempdb_mssql_3.ndf
tempdb_mssql_4.ndf
tempdb_mssql_5.ndf
tempdb_mssql_6.ndf
tempdb_mssql_7.ndf
tempdb_mssql_8.ndf
templog.ldf
```

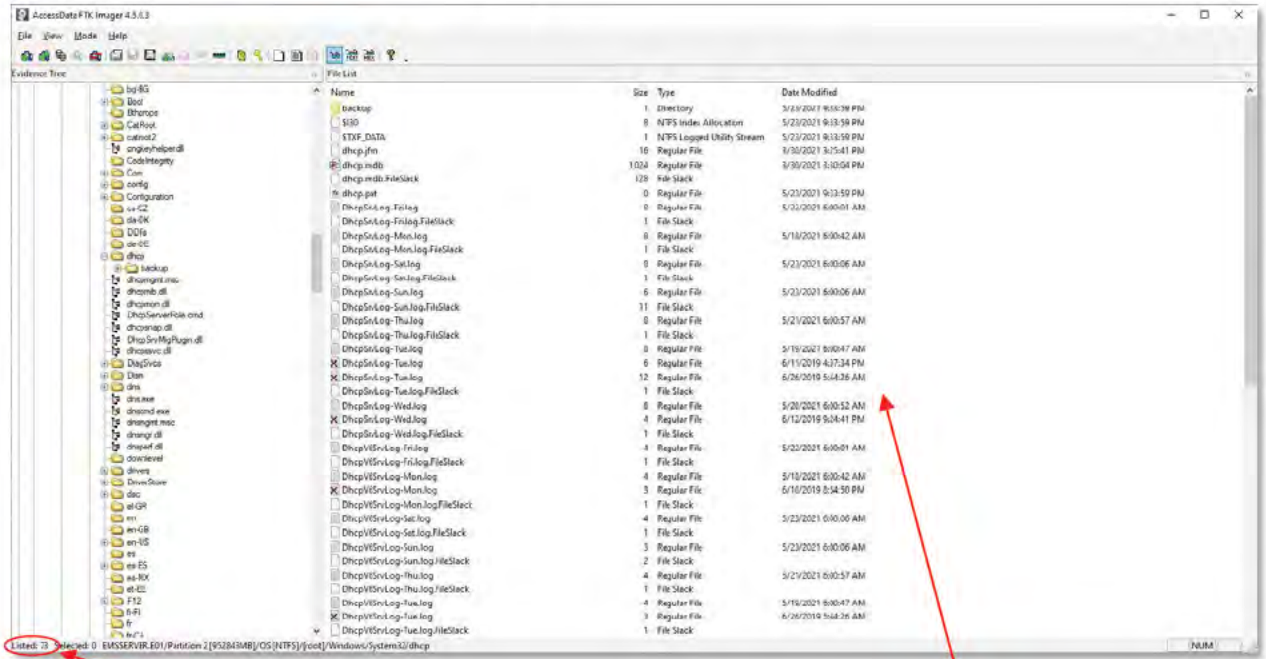
```
00 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 30 0
Cursor pos = 0
Listed: 22  Selected: 0  EMSSERVER_v2.E01/Partition 4 [952740MB]/EMS [NTFS]/[root]/Program Files/Microsoft SQL Server/MSSQL13.MSSQLSERVER/MSSQL/DATA    NUM
```

The Entire Database Directory is gone along with all files that were in it.

Server DHCP Log Files Missing/Overwritten

Purpose: *DHCP Log Files can show evidence regarding computers or other devices being connected to the network.*

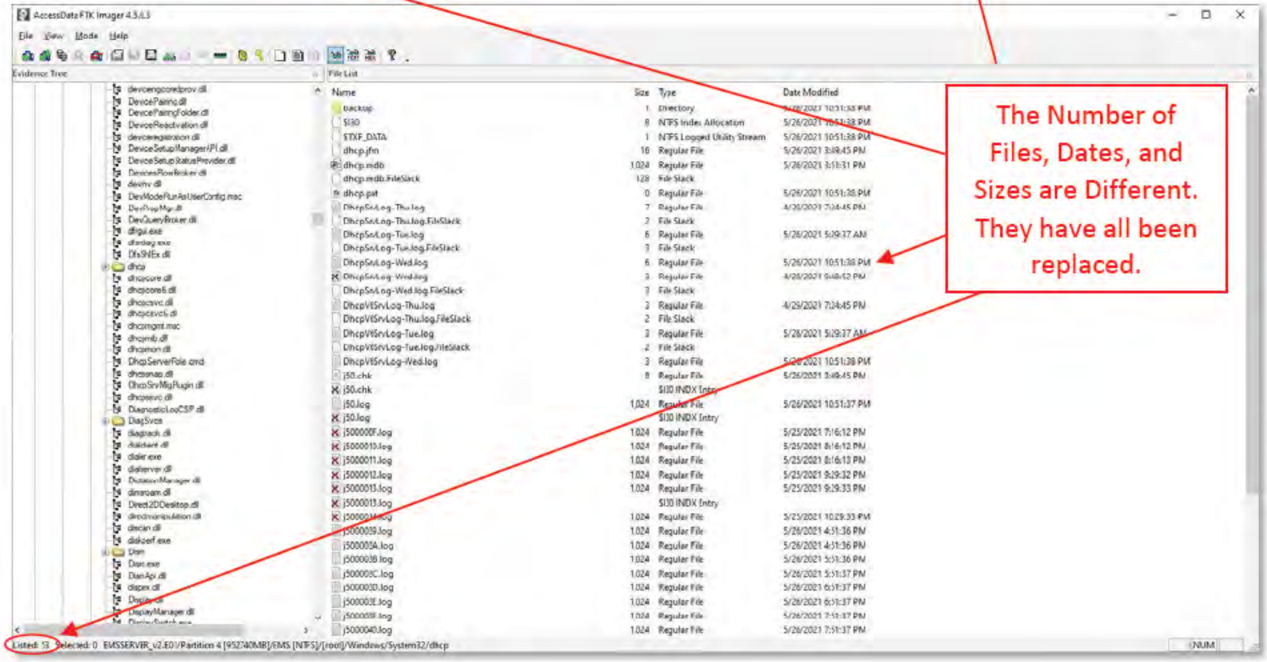
Figure 29 - EMS Server (5.11-CO) DHCP Log Files Before



Name	Size	Type	Date Modified
backup	1	Directory	5/23/2021 9:33:39 PM
$I30	8	NTFS Index Allocation	5/23/2021 9:13:59 PM
$TXF_DATA	1	NTFS Logged Utility Stream	5/23/2021 9:13:59 PM
dhcp.jfm	16	Regular File	3/30/2021 3:25:41 PM
dhcp.mdb	1,024	Regular File	3/30/2021 3:30:04 PM
dhcp.mdb.FileSlack	128	File Slack	
dhcp.pat	0	Regular File	5/23/2021 9:13:59 PM
DhcpSrvLog-Fri.log	8	Regular File	5/22/2021 6:00:01 AM
DhcpSrvLog-Fri.log.FileSlack	1	File Slack	
DhcpSrvLog-Mon.log	8	Regular File	5/18/2021 6:00:42 AM
DhcpSrvLog-Mon.log.FileSlack	1	File Slack	
DhcpSrvLog-Sat.log	8	Regular File	5/23/2021 6:00:06 AM
DhcpSrvLog-Sat.log.FileSlack	1	File Slack	
DhcpSrvLog-Sun.log	6	Regular File	5/23/2021 6:00:06 AM
DhcpSrvLog-Sun.log.FileSlack	11	File Slack	
DhcpSrvLog-Thu.log	8	Regular File	5/21/2021 6:00:57 AM
DhcpSrvLog-Thu.log.FileSlack	1	File Slack	
DhcpSrvLog-Tue.log	8	Regular File	5/19/2021 6:00:47 AM
DhcpSrvLog-Tue.log	6	Regular File	6/11/2019 4:37:34 PM
DhcpSrvLog-Tue.log	12	Regular File	6/26/2019 5:44:26 AM
DhcpSrvLog-Tue.log.FileSlack	1	File Slack	
DhcpSrvLog-Wed.log	8	Regular File	5/20/2021 6:00:52 AM
DhcpSrvLog-Wed.log	4	Regular File	6/12/2019 9:34:41 PM
DhcpSrvLog-Wed.log.FileSlack	1	File Slack	
DhcpV6SrvLog-Fri.log	4	Regular File	5/22/2021 6:00:01 AM
DhcpV6SrvLog-Fri.log.FileSlack	1	File Slack	
DhcpV6SrvLog-Mon.log	4	Regular File	5/18/2021 6:00:42 AM
DhcpV6SrvLog-Mon.log	3	Regular File	6/10/2019 8:54:50 PM
DhcpV6SrvLog-Mon.log.FileSlack	1	File Slack	
DhcpV6SrvLog-Sat.log	4	Regular File	5/23/2021 6:00:06 AM
DhcpV6SrvLog-Sat.log.FileSlack	1	File Slack	
DhcpV6SrvLog-Sun.log	3	Regular File	5/23/2021 6:00:06 AM
DhcpV6SrvLog-Sun.log.FileSlack	2	File Slack	
DhcpV6SrvLog-Thu.log	4	Regular File	5/21/2021 6:00:57 AM
DhcpV6SrvLog-Thu.log.FileSlack	1	File Slack	
DhcpV6SrvLog-Tue.log	4	Regular File	5/19/2021 6:00:47 AM
DhcpV6SrvLog-Tue.log	3	Regular File	6/26/2019 5:44:26 AM
DhcpV6SrvLog-Tue.log.FileSlack	1	File Slack	

Listed: 73 Selected: 0 EMSSERVER.E01/Partition 2 [952843MB]/OS [NTFS]/[root]/Windows/System32/dhcp

Figure 30 - EMS Server (5.13) DHCP Log Files After



Name	Size	Type	Date Modified
backup	1	Directory	5/26/2021 10:51:38 PM
$I30	8	NTFS Index Allocation	5/26/2021 10:51:38 PM
$TXF_DATA	1	NTFS Logged Utility Stream	5/26/2021 10:51:38 PM
dhcp.jfm	16	Regular File	5/26/2021 3:49:45 PM
dhcp.mdb	1,024	Regular File	5/26/2021 3:51:31 PM
dhcp.mdb.FileSlack	128	File Slack	
dhcp.pat	0	Regular File	5/26/2021 10:51:38 PM
DhcpSrvLog-Thu.log	7	Regular File	4/29/2021 7:24:45 PM
DhcpSrvLog-Thu.log.FileSlack	2	File Slack	
DhcpSrvLog-Tue.log	6	Regular File	5/26/2021 5:29:37 AM
DhcpSrvLog-Tue.log.FileSlack	3	File Slack	
DhcpSrvLog-Wed.log	6	Regular File	5/26/2021 10:51:38 PM
DhcpSrvLog-Wed.log	3	Regular File	4/28/2021 9:48:52 PM
DhcpSrvLog-Wed.log.FileSlack	7	File Slack	
DhcpV6SrvLog-Thu.log	3	Regular File	4/29/2021 7:24:45 PM
DhcpV6SrvLog-Thu.log.FileSlack	2	File Slack	
DhcpV6SrvLog-Tue.log	3	Regular File	5/26/2021 5:29:37 AM
DhcpV6SrvLog-Tue.log.FileSlack	2	File Slack	
DhcpV6SrvLog-Wed.log	3	Regular File	5/26/2021 10:51:38 PM
j50.chk	8	Regular File	5/26/2021 3:49:45 PM
j50.chk		$I30 INDX Entry	
j50.log	1,024	Regular File	5/26/2021 10:51:37 PM
j50.log		$I30 INDX Entry	
j500000F.log	1,024	Regular File	5/25/2021 7:16:12 PM
j5000010.log	1,024	Regular File	5/25/2021 8:16:12 PM
j5000011.log	1,024	Regular File	5/25/2021 8:16:13 PM
j5000012.log	1,024	Regular File	5/25/2021 9:29:32 PM
j5000013.log	1,024	Regular File	5/25/2021 9:29:33 PM
j5000013.log		$I30 INDX Entry	
j5000014.log	1,024	Regular File	5/25/2021 10:29:33 PM
j5000039.log	1,024	Regular File	5/26/2021 4:51:36 PM
j500003A.log	1,024	Regular File	5/26/2021 4:51:36 PM
j500003B.log	1,024	Regular File	5/26/2021 5:51:36 PM
j500003C.log	1,024	Regular File	5/26/2021 5:51:37 PM
j500003D.log	1,024	Regular File	5/26/2021 6:51:37 PM
j500003E.log	1,024	Regular File	5/26/2021 6:51:37 PM
j500003F.log	1,024	Regular File	5/26/2021 7:51:37 PM
j5000040.log	1,024	Regular File	5/26/2021 7:51:37 PM

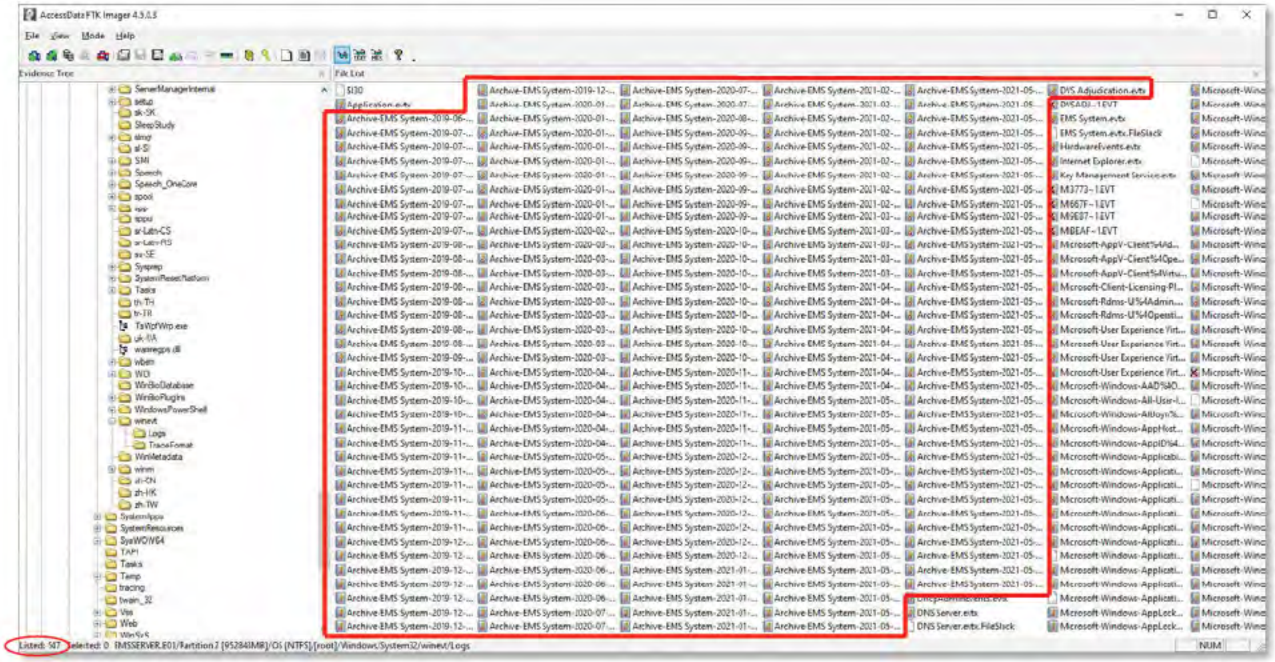
Listed: 53 Selected: 0 EMSSERVER_v2.E01/Partition 4 [952740MB]/EMS [NTFS]/[root]/Windows/System32/dhcp

The Number of Files, Dates, and Sizes are Different. They have all been replaced.

Server Event Logs Missing/Overwritten

Purpose: *These Dominion Log Files keep track of election/project-related activity. The Windows Server event logs outside the red box keep track of much of the activity on the server.*

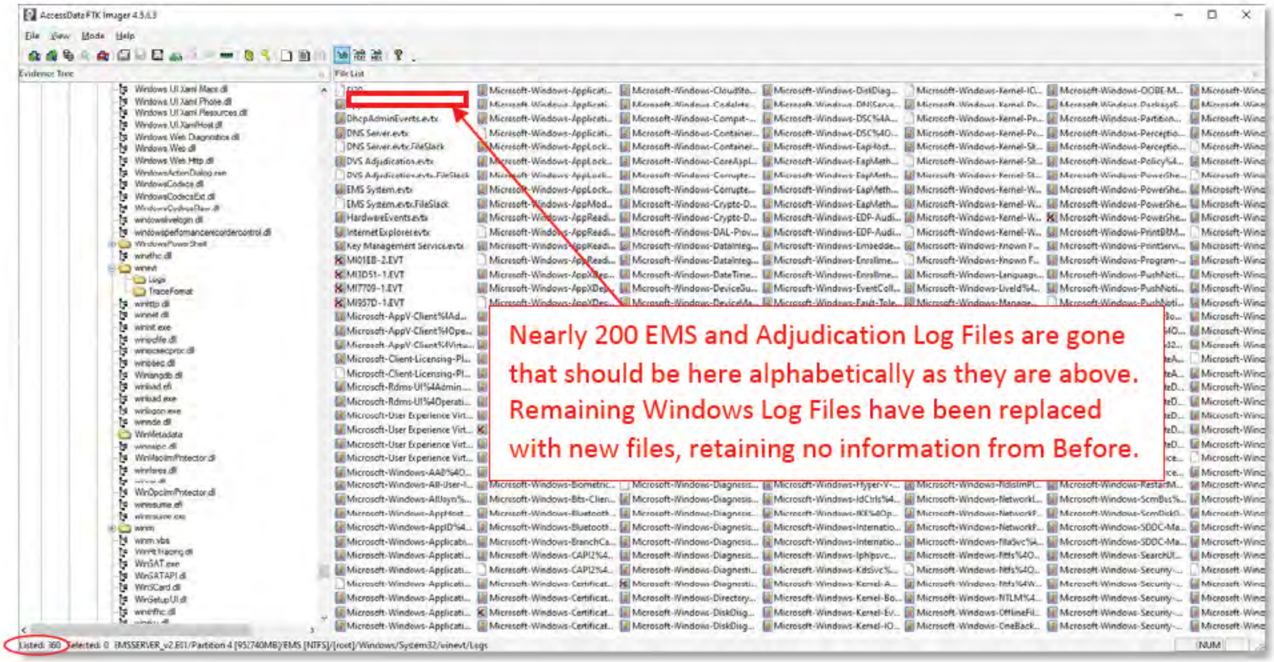
Figure 31 - EMS Server (5.11-CO) Event Logs Before



AccessData FTK Imager 4.5.0.3

Listed: 507 Selected: 0 EMSSERVER.E01/Partition 2 [95284MB]/OS (NTFS)/[root]/Windows/System32/winevt/Logs

Figure 32 - EMS Server (5.13) Event Logs After



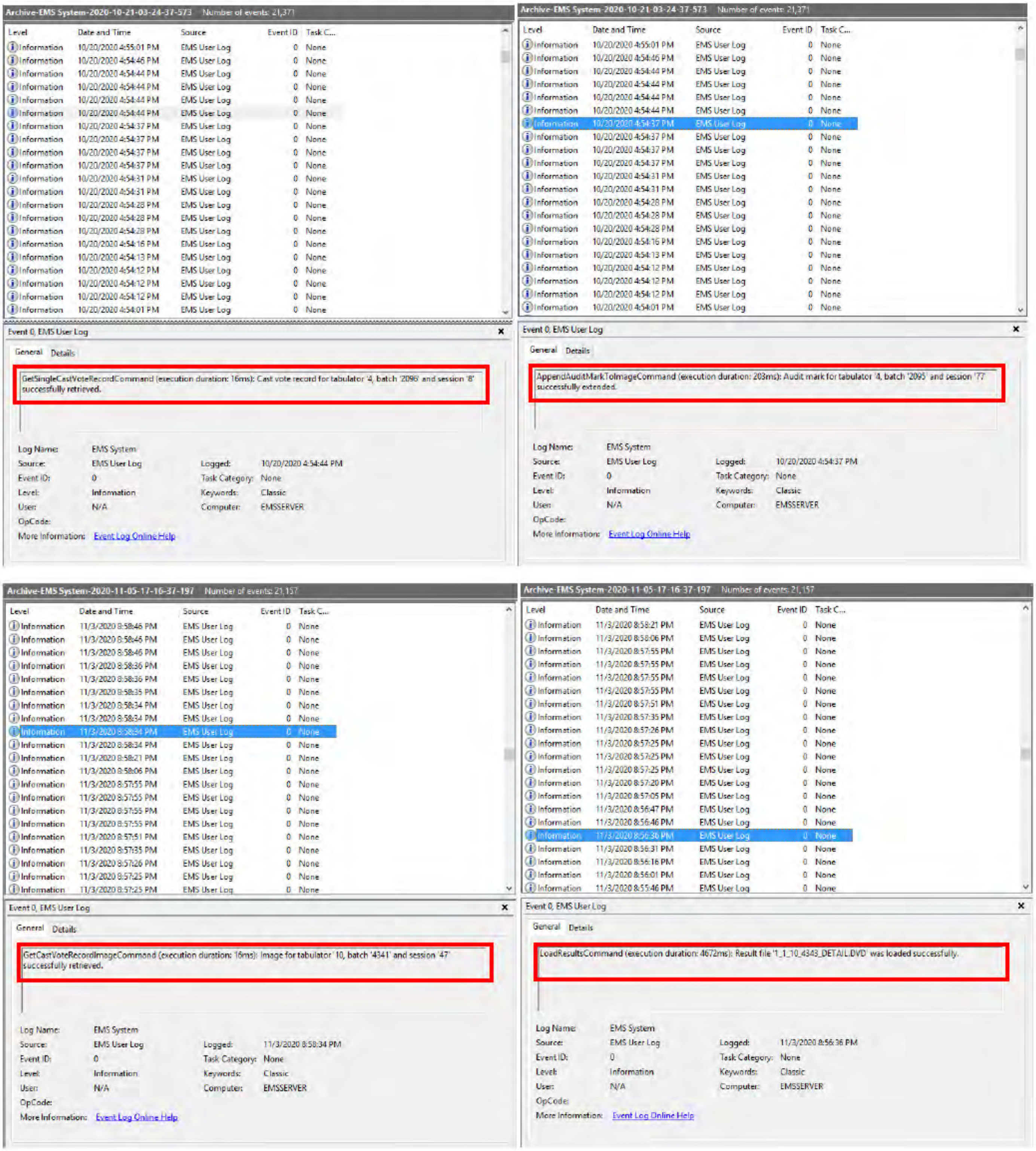
AccessData FTK Imager 4.5.0.3

Nearly 200 EMS and Adjudication Log Files are gone that should be here alphabetically as they are above. Remaining Windows Log Files have been replaced with new files, retaining no information from Before.

Listed: 360 Selected: 0 EMSSERVER_v2.E01/Partition 4 [952740MB]/EMS [NTFS]/[root]/Windows/System32/winevt/Logs

Below are some screen shots of the kind of Election-Related information (such as cast vote records, audit marks, image retrievals, result file loads, etc.) in the EMS Archive Logs that are missing After the Dominion Update:

Figure 33 - Examples of Election Data Missing After Update



```
Archive-EMS System-2020-10-21-03-24-37-573   Number of events: 21,371

Level        Date and Time           Source        Event ID  Task C...
Information  10/20/2020 4:55:01 PM   EMS User Log  0         None
Information  10/20/2020 4:54:46 PM   EMS User Log  0         None
Information  10/20/2020 4:54:44 PM   EMS User Log  0         None
Information  10/20/2020 4:54:44 PM   EMS User Log  0         None
Information  10/20/2020 4:54:44 PM   EMS User Log  0         None
Information  10/20/2020 4:54:44 PM   EMS User Log  0         None
Information  10/20/2020 4:54:37 PM   EMS User Log  0         None
Information  10/20/2020 4:54:37 PM   EMS User Log  0         None
Information  10/20/2020 4:54:37 PM   EMS User Log  0         None
Information  10/20/2020 4:54:37 PM   EMS User Log  0         None
Information  10/20/2020 4:54:31 PM   EMS User Log  0         None
Information  10/20/2020 4:54:31 PM   EMS User Log  0         None
Information  10/20/2020 4:54:28 PM   EMS User Log  0         None
Information  10/20/2020 4:54:28 PM   EMS User Log  0         None
Information  10/20/2020 4:54:28 PM   EMS User Log  0         None
Information  10/20/2020 4:54:16 PM   EMS User Log  0         None
Information  10/20/2020 4:54:13 PM   EMS User Log  0         None
Information  10/20/2020 4:54:12 PM   EMS User Log  0         None
Information  10/20/2020 4:54:12 PM   EMS User Log  0         None
Information  10/20/2020 4:54:12 PM   EMS User Log  0         None
Information  10/20/2020 4:54:01 PM   EMS User Log  0         None

Event 0, EMS User Log
General  Details

GetSingleCastVoteRecordCommand (execution duration: 16ms): Cast vote record for tabulator '4, batch '2096' and session '8'
successfully retrieved.

Log Name:   EMS System
Source:     EMS User Log       Logged:         10/20/2020 4:54:44 PM
Event ID:   0                  Task Category:  None
Level:      Information        Keywords:       Classic
User:       N/A                Computer:       EMSSERVER
OpCode:
More Information:  Event Log Online Help
```

```
Archive-EMS System-2020-10-21-03-24-37-573   Number of events: 21,371

Level        Date and Time           Source        Event ID  Task C...
Information  10/20/2020 4:55:01 PM   EMS User Log  0         None
Information  10/20/2020 4:54:46 PM   EMS User Log  0         None
Information  10/20/2020 4:54:44 PM   EMS User Log  0         None
Information  10/20/2020 4:54:44 PM   EMS User Log  0         None
Information  10/20/2020 4:54:44 PM   EMS User Log  0         None
Information  10/20/2020 4:54:44 PM   EMS User Log  0         None
Information  10/20/2020 4:54:37 PM   EMS User Log  0         None
Information  10/20/2020 4:54:37 PM   EMS User Log  0         None
Information  10/20/2020 4:54:37 PM   EMS User Log  0         None
Information  10/20/2020 4:54:37 PM   EMS User Log  0         None
Information  10/20/2020 4:54:31 PM   EMS User Log  0         None
Information  10/20/2020 4:54:31 PM   EMS User Log  0         None
Information  10/20/2020 4:54:28 PM   EMS User Log  0         None
Information  10/20/2020 4:54:28 PM   EMS User Log  0         None
Information  10/20/2020 4:54:28 PM   EMS User Log  0         None
Information  10/20/2020 4:54:16 PM   EMS User Log  0         None
Information  10/20/2020 4:54:13 PM   EMS User Log  0         None
Information  10/20/2020 4:54:12 PM   EMS User Log  0         None
Information  10/20/2020 4:54:12 PM   EMS User Log  0         None
Information  10/20/2020 4:54:12 PM   EMS User Log  0         None
Information  10/20/2020 4:54:01 PM   EMS User Log  0         None

Event 0, EMS User Log
General  Details

AppendAuditMarkToImageCommand (execution duration: 203ms): Audit mark for tabulator '4, batch '2095' and session '77'
successfully extended.

Log Name:   EMS System
Source:     EMS User Log       Logged:         10/20/2020 4:54:37 PM
Event ID:   0                  Task Category:  None
Level:      Information        Keywords:       Classic
User:       N/A                Computer:       EMSSERVER
OpCode:
More Information:  Event Log Online Help
```

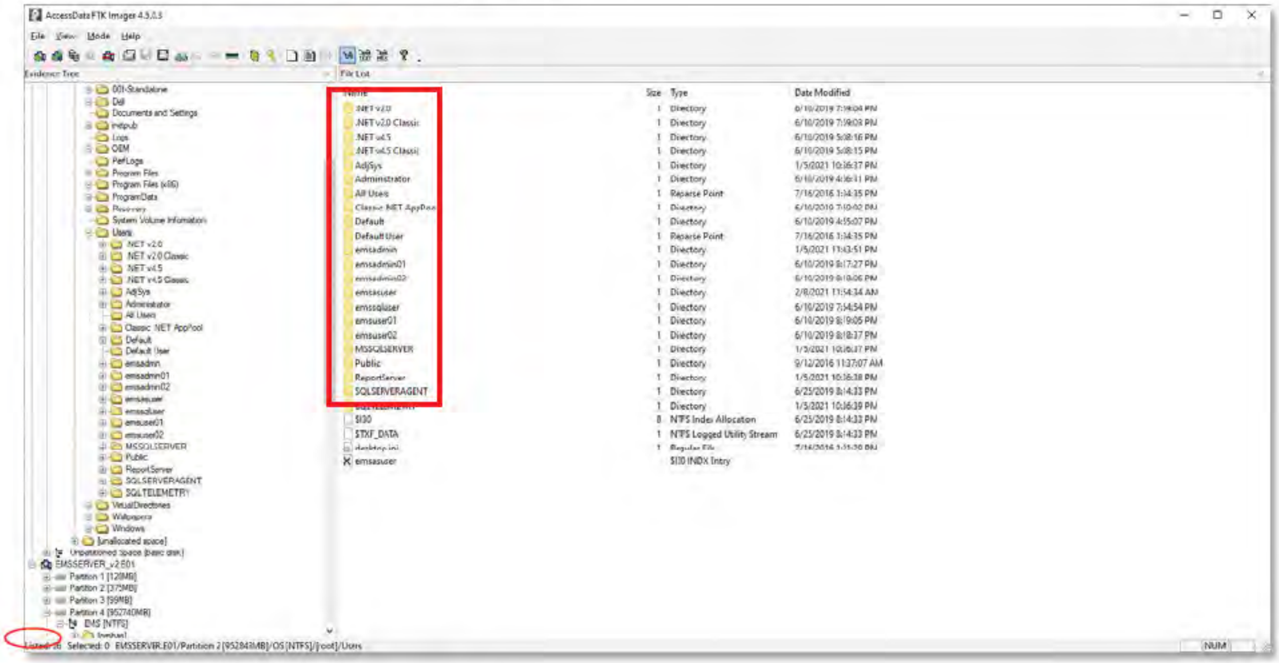
```
Archive-EMS System-2020-11-05-17-16-37-197   Number of events: 21,157

Level        Date and Time          Source        Event ID  Task C...
Information  11/3/2020 8:58:46 PM   EMS User Log  0         None
Information  11/3/2020 8:58:46 PM   EMS User Log  0         None
Information  11/3/2020 8:58:46 PM   EMS User Log  0         None
Information  11/3/2020 8:58:36 PM   EMS User Log  0         None
Information  11/3/2020 8:58:36 PM   EMS User Log  0         None
Information  11/3/2020 8:58:35 PM   EMS User Log  0         None
Information  11/3/2020 8:58:34 PM   EMS User Log  0         None
Information  11/3/2020 8:58:34 PM   EMS User Log  0         None
Information  11/3/2020 8:58:34 PM   EMS User Log  0         None
Information  11/3/2020 8:58:34 PM   EMS User Log  0         None
Information  11/3/2020 8:58:21 PM   EMS User Log  0         None
Information  11/3/2020 8:58:06 PM   EMS User Log  0         None
Information  11/3/2020 8:57:55 PM   EMS User Log  0         None
Information  11/3/2020 8:57:55 PM   EMS User Log  0         None
Information  11/3/2020 8:57:55 PM   EMS User Log  0         None
Information  11/3/2020 8:57:55 PM   EMS User Log  0         None
Information  11/3/2020 8:57:51 PM   EMS User Log  0         None
Information  11/3/2020 8:57:35 PM   EMS User Log  0         None
Information  11/3/2020 8:57:26 PM   EMS User Log  0         None
Information  11/3/2020 8:57:25 PM   EMS User Log  0         None
Information  11/3/2020 8:57:25 PM   EMS User Log  0         None

Event 0, EMS User Log
General  Details

GetCastVoteRecordImageCommand (execution duration: 16ms): Image for tabulator '10, batch '4341' and session '47'
successfully retrieved.

Log Name:   EMS System
Source:     EMS User Log       Logged:         11/3/2020 8:58:34 PM
Event ID:   0                  Task Category:  None
Level:      Information        Keywords:       Classic
User:       N/A                Computer:       EMSSERVER
OpCode:
More Information:  Event Log Online Help
```

```
Archive-EMS System-2020-11-05-17-16-37-197   Number of events: 21,157

Level        Date and Time          Source        Event ID  Task C...
Information  11/3/2020 8:58:21 PM   EMS User Log  0         None
Information  11/3/2020 8:58:06 PM   EMS User Log  0         None
Information  11/3/2020 8:57:55 PM   EMS User Log  0         None
Information  11/3/2020 8:57:55 PM   EMS User Log  0         None
Information  11/3/2020 8:57:55 PM   EMS User Log  0         None
Information  11/3/2020 8:57:55 PM   EMS User Log  0         None
Information  11/3/2020 8:57:51 PM   EMS User Log  0         None
Information  11/3/2020 8:57:35 PM   EMS User Log  0         None
Information  11/3/2020 8:57:26 PM   EMS User Log  0         None
Information  11/3/2020 8:57:25 PM   EMS User Log  0         None
Information  11/3/2020 8:57:25 PM   EMS User Log  0         None
Information  11/3/2020 8:57:25 PM   EMS User Log  0         None
Information  11/3/2020 8:57:20 PM   EMS User Log  0         None
Information  11/3/2020 8:57:05 PM   EMS User Log  0         None
Information  11/3/2020 8:56:47 PM   EMS User Log  0         None
Information  11/3/2020 8:56:46 PM   EMS User Log  0         None
Information  11/3/2020 8:56:36 PM   EMS User Log  0         None
Information  11/3/2020 8:56:31 PM   EMS User Log  0         None
Information  11/3/2020 8:56:16 PM   EMS User Log  0         None
Information  11/3/2020 8:56:01 PM   EMS User Log  0         None
Information  11/3/2020 8:55:46 PM   EMS User Log  0         None

Event 0, EMS User Log
General  Details

LoadResultsCommand (execution duration: 4672ms): Result file '1_1_10_4343_DETAIL.DVD' was loaded successfully.

Log Name:   EMS System
Source:     EMS User Log       Logged:         11/3/2020 8:56:36 PM
Event ID:   0                  Task Category:  None
Level:      Information        Keywords:       Classic
User:       N/A                Computer:       EMSSERVER
OpCode:
More Information:  Event Log Online Help
```

Server System Users are Missing

Purpose: *These folders store the information for each user account on the server.*

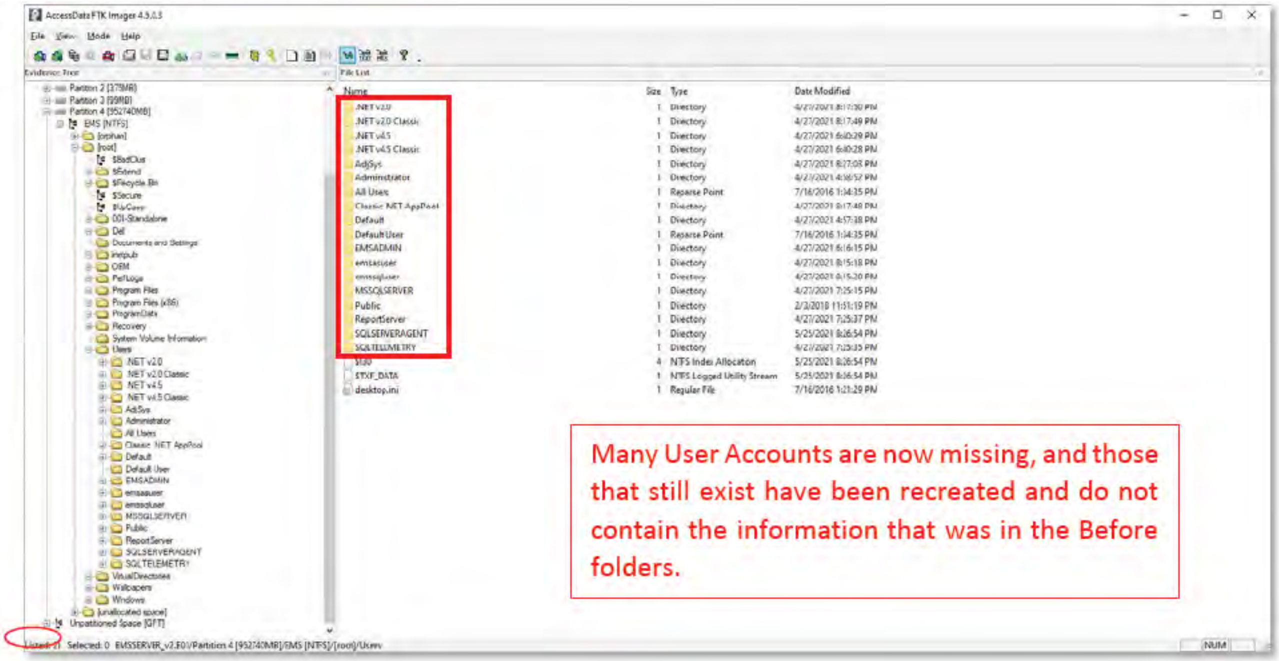
Figure 34 - EMS Server (5.11-CO) System Users Before



Name	Size	Type	Date Modified
.NET v2.0	1	Directory	6/10/2019 7:19:04 PM
.NET v2.0 Classic	1	Directory	6/10/2019 7:19:03 PM
.NET v4.5	1	Directory	6/10/2019 5:08:16 PM
.NET v4.5 Classic	1	Directory	6/10/2019 5:08:15 PM
AdjSys	1	Directory	1/5/2021 10:16:37 PM
Administrator	1	Directory	6/10/2019 4:16:11 PM
All Users	1	Reparse Point	7/16/2016 1:14:35 PM
Classic .NET AppPool	1	Directory	6/10/2019 7:10:02 PM
Default	1	Directory	6/10/2019 4:15:07 PM
Default User	1	Reparse Point	7/16/2016 1:14:35 PM
emsadmin	1	Directory	1/5/2021 11:43:51 PM
emsadmin01	1	Directory	6/10/2019 8:17:27 PM
emsadmin02	1	Directory	6/10/2019 8:10:06 PM
emsasuser	1	Directory	2/8/2021 11:54:34 AM
emssqluser	1	Directory	6/10/2019 7:54:54 PM
emsuser01	1	Directory	6/10/2019 8:19:05 PM
emsuser02	1	Directory	6/10/2019 8:18:37 PM
MSSQLSERVER	1	Directory	1/5/2021 10:16:37 PM
Public	1	Directory	9/12/2016 11:37:07 AM
ReportServer	1	Directory	1/5/2021 10:16:38 PM
SQLSERVERAGENT	1	Directory	6/25/2019 8:14:33 PM
SQLTELEMETRY	1	Directory	1/5/2021 10:16:39 PM
$I30	8	NTFS Index Allocation	6/25/2019 8:14:33 PM
$TXF_DATA	1	NTFS Logged Utility Stream	6/25/2019 8:14:33 PM
desktop.ini	1	Regular File	7/16/2016 1:21:30 PM
emsasuser		$I30 INDX Entry	

Listed: 26 Selected: 0 EMSSERVER.E01/Partition 2 [952843MB]/OS [NTFS]/[root]/Users

Figure 35 - EMS Server (5.13) System Users After



Name	Size	Type	Date Modified
.NET v2.0	1	Directory	4/27/2021 8:17:50 PM
.NET v2.0 Classic	1	Directory	4/27/2021 8:17:49 PM
.NET v4.5	1	Directory	4/27/2021 6:40:29 PM
.NET v4.5 Classic	1	Directory	4/27/2021 6:40:28 PM
AdjSys	1	Directory	4/27/2021 8:27:03 PM
Administrator	1	Directory	4/27/2021 4:38:57 PM
All Users	1	Reparse Point	7/16/2016 1:14:35 PM
Classic .NET AppPool	1	Directory	4/27/2021 8:17:48 PM
Default	1	Directory	4/27/2021 4:57:38 PM
Default User	1	Reparse Point	7/16/2016 1:14:35 PM
EMSADMIN	1	Directory	4/27/2021 6:16:15 PM
emsasuser	1	Directory	4/27/2021 8:15:18 PM
emssqluser	1	Directory	4/27/2021 8:15:20 PM
MSSQLSERVER	1	Directory	4/27/2021 7:25:15 PM
Public	1	Directory	2/3/2018 11:51:19 PM
ReportServer	1	Directory	4/27/2021 7:25:37 PM
SQLSERVERAGENT	1	Directory	5/25/2021 8:26:54 PM
SQLTELEMETRY	1	Directory	4/27/2021 7:25:35 PM
$I30	4	NTFS Index Allocation	5/25/2021 8:26:54 PM
$TXF_DATA	1	NTFS Logged Utility Stream	5/25/2021 8:26:54 PM
desktop.ini	1	Regular File	7/16/2016 1:21:29 PM

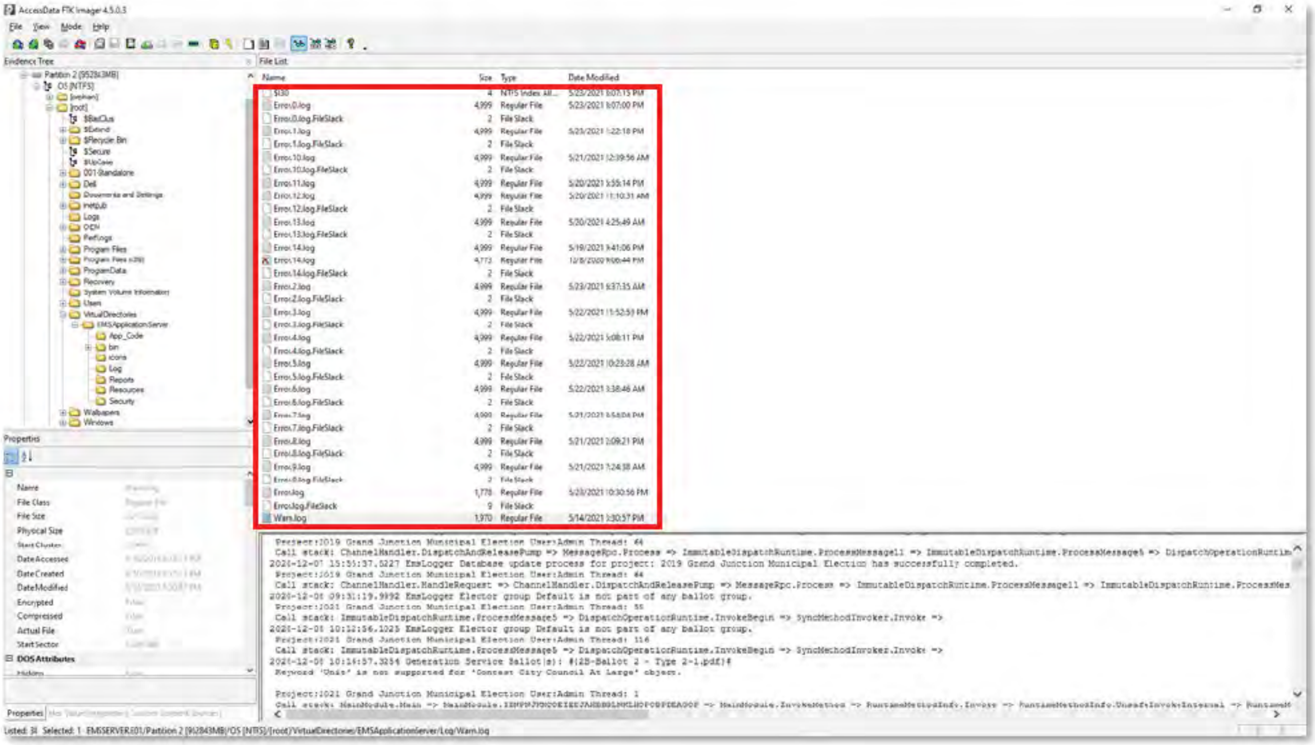
Listed: 21 Selected: 0 EMSSERVER_v2.E01/Partition 4 [952740MB]/EMS [NTFS]/[root]/Users

Many User Accounts are now missing, and those that still exist have been recreated and do not contain the information that was in the Before folders.

Server Virtual Directories Log Files Missing

Purpose: *These are the Log Files that contain information, warnings, and errors relating to the Website Server as the server processes election projects that have been set up.*

Figure 36 - EMS Server (5.11-CO) Virtual Directory Log Files Before

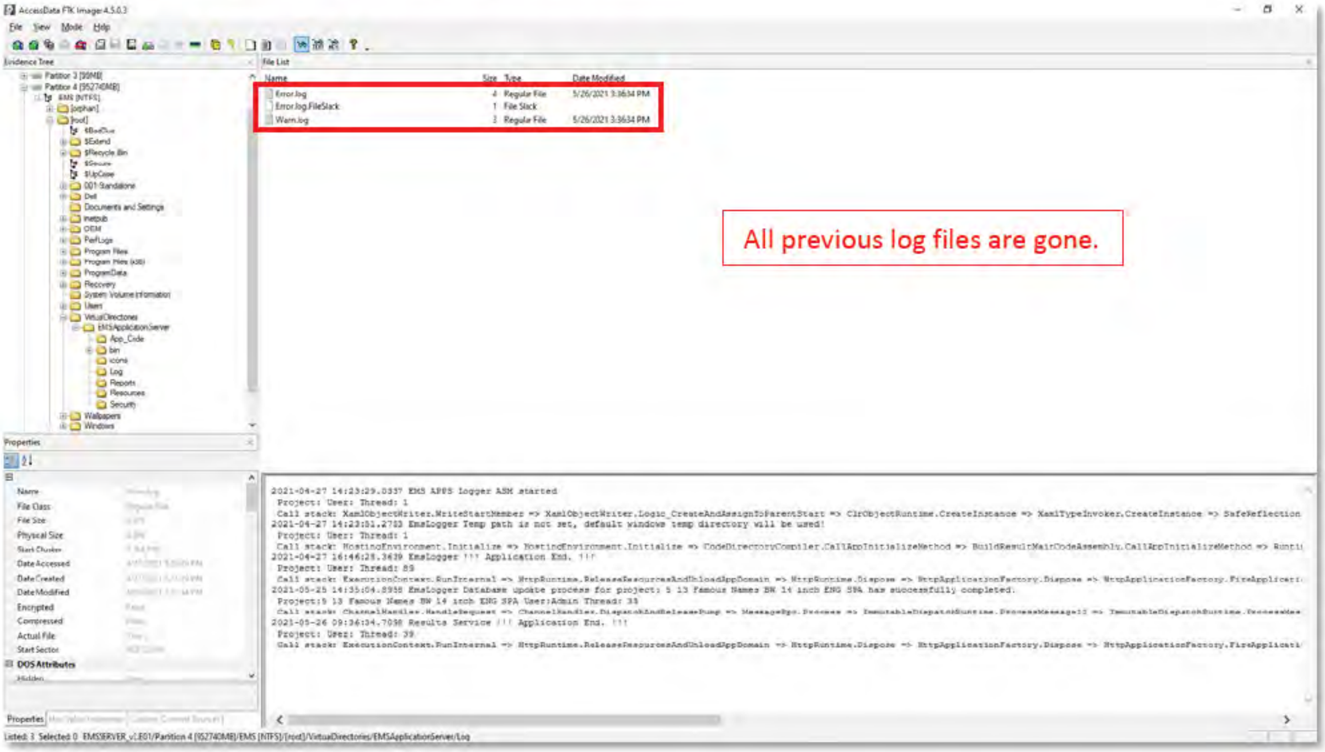


Name	Size	Type	Date Modified
$I30	4	NTFS Index All...	5/23/2021 8:07:15 PM
Error.0.log	4,999	Regular File	5/23/2021 8:07:00 PM
Error.0.log.FileSlack	2	File Slack	
Error.1.log	4,999	Regular File	5/23/2021 1:22:18 PM
Error.1.log.FileSlack	2	File Slack	
Error.10.log	4,999	Regular File	5/21/2021 12:39:56 AM
Error.10.log.FileSlack	2	File Slack	
Error.11.log	4,999	Regular File	5/20/2021 5:55:14 PM
Error.12.log	4,999	Regular File	5/20/2021 11:10:31 AM
Error.12.log.FileSlack	2	File Slack	
Error.13.log	4,999	Regular File	5/20/2021 4:25:49 AM
Error.13.log.FileSlack	2	File Slack	
Error.14.log	4,999	Regular File	5/19/2021 9:41:06 PM
Error.14.log	4,773	Regular File	12/8/2020 9:06:44 PM
Error.14.log.FileSlack	2	File Slack	
Error.2.log	4,999	Regular File	5/23/2021 6:37:35 AM
Error.2.log.FileSlack	2	File Slack	
Error.3.log	4,999	Regular File	5/22/2021 11:52:53 PM
Error.3.log.FileSlack	2	File Slack	
Error.4.log	4,999	Regular File	5/22/2021 5:08:11 PM
Error.4.log.FileSlack	2	File Slack	
Error.5.log	4,999	Regular File	5/22/2021 10:23:28 AM
Error.5.log.FileSlack	2	File Slack	
Error.6.log	4,999	Regular File	5/22/2021 3:38:46 AM
Error.6.log.FileSlack	2	File Slack	
Error.7.log	4,999	Regular File	5/21/2021 8:54:04 PM
Error.7.log.FileSlack	2	File Slack	
Error.8.log	4,999	Regular File	5/21/2021 2:09:21 PM
Error.8.log.FileSlack	2	File Slack	
Error.9.log	4,999	Regular File	5/21/2021 7:24:38 AM
Error.9.log.FileSlack	2	File Slack	
Error.log	1,778	Regular File	5/23/2021 10:30:56 PM
Error.log.FileSlack	9	File Slack	
Warn.log	1,970	Regular File	5/14/2021 3:30:57 PM

```
 Project:2019 Grand Junction Municipal Election User:Admin Thread: 44
 Call stack: ChannelHandler.DispatchAndReleasePump => MessageRpc.Process => ImmutableDispatchRuntime.ProcessMessage11 => ImmutableDispatchRuntime.ProcessMessage5 => DispatchOperationRuntim
2020-12-07 15:55:37.5227 EmsLogger Database update process for project: 2019 Grand Junction Municipal Election has successfully completed.
 Project:2019 Grand Junction Municipal Election User:Admin Thread: 44
 Call stack: ChannelHandler.HandleRequest => ChannelHandler.DispatchAndReleasePump => MessageRpc.Process => ImmutableDispatchRuntime.ProcessMessage11 => ImmutableDispatchRuntime.ProcessMes
2020-12-08 09:31:19.9992 EmsLogger Elector group Default is not part of any ballot group.
 Project:2021 Grand Junction Municipal Election User:Admin Thread: 55
 Call stack: ImmutableDispatchRuntime.ProcessMessage5 => DispatchOperationRuntime.InvokeBegin => SyncMethodInvoker.Invoke =>
2020-12-08 10:12:56.1025 EmsLogger Elector group Default is not part of any ballot group.
 Project:2021 Grand Junction Municipal Election User:Admin Thread: 116
 Call stack: ImmutableDispatchRuntime.ProcessMessage5 => DispatchOperationRuntime.InvokeBegin => SyncMethodInvoker.Invoke =>
2020-12-08 10:14:57.3254 Generation Service Ballot(s): #(2B-Ballot 2 - Type 2-1.pdf)#
 Keyword 'Unit' is not supported for 'Contest City Council At Large' object.

 Project:2021 Grand Junction Municipal Election User:Admin Thread: 1
 Call stack: MainModule.Main => MainModule.IINPPJPNCOEIEEJAHBBGLMKLHOPOBPDEAGOF => MainModule.InvokeMethod => RuntimeMethodInfo.Invoke => RuntimeMethodInfo.UnsafeInvokeInternal => RuntimeM
```

Listed: 31 Selected: 1 EMSSERVER.E01/Partition 2 [952843MB]/OS [NTFS]/[root]/VirtualDirectories/EMSApplicationServer/Log/Warn.log

Figure 37 - EMS Server (5.13) Virtual Directory Log Files After



Name	Size	Type	Date Modified
Error.log	4	Regular File	5/26/2021 3:36:34 PM
Error.log.FileSlack	1	File Slack	
Warn.log	3	Regular File	5/26/2021 3:36:34 PM

All previous log files are gone.

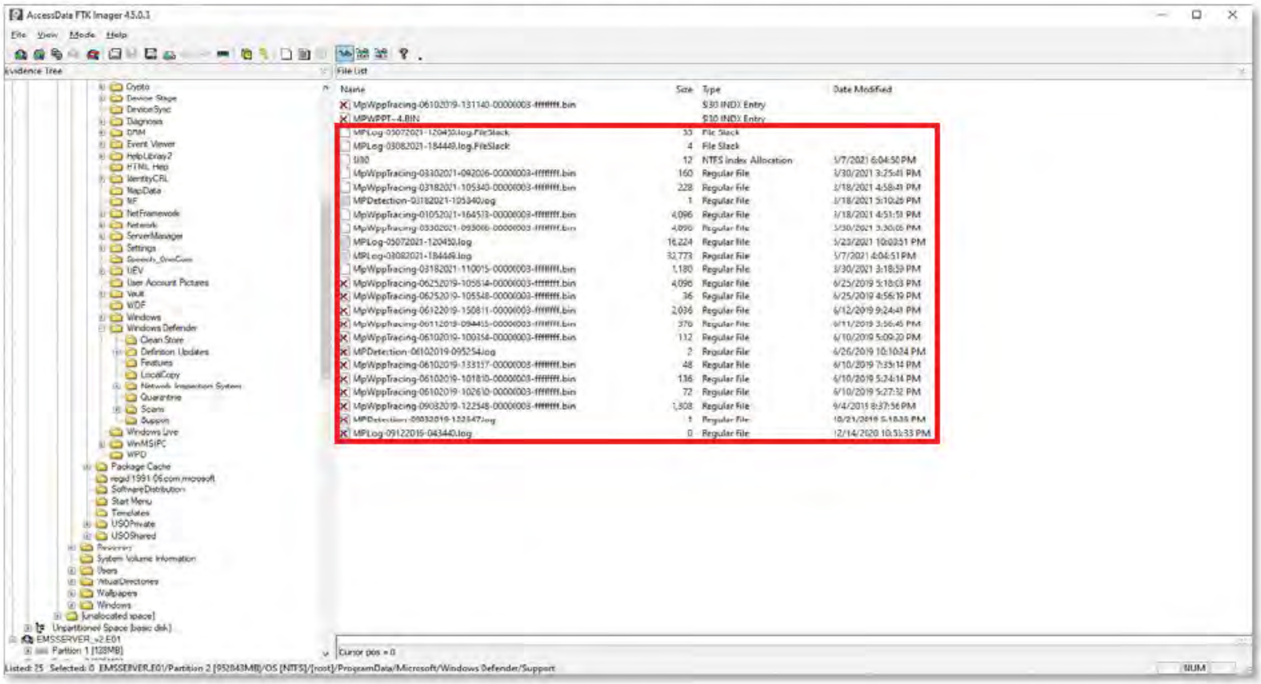
```
2021-04-27 14:23:29.0337 EMS APPS Logger ASM started
 Project: User: Thread: 1
 Call stack: XamlObjectWriter.WriteStartMember => XamlObjectWriter.Logic_CreateAndAssignToParentStart => ClrObjectRuntime.CreateInstance => XamlTypeInvoker.CreateInstance => SafeReflection
2021-04-27 14:23:31.2703 EmsLogger Temp path is not set, default windows temp directory will be used!
 Project: User: Thread: 1
 Call stack: HostingEnvironment.Initialize => HostingEnvironment.Initialize => CodeDirectoryCompiler.CallAppInitializeMethod => BuildResultMainCodeAssembly.CallAppInitializeMethod => Runti
2021-04-27 16:46:28.3639 EmsLogger !!! Application End. !!!
 Project: User: Thread: 89
 Call stack: ExecutionContext.RunInternal => HttpRuntime.ReleaseResourcesAndUnloadAppDomain => HttpRuntime.Dispose => HttpApplicationFactory.Dispose => HttpApplicationFactory.FireApplicati
2021-05-25 14:35:04.8958 EmsLogger Database update process for project: 5 13 Famous Names BW 14 inch ENG SPA has successfully completed.
 Project:5 13 Famous Names BW 14 inch ENG SPA User:Admin Thread: 35
 Call stack: ChannelHandler.HandleRequest => ChannelHandler.DispatchAndReleasePump => MessageRpc.Process => ImmutableDispatchRuntime.ProcessMessage11 => ImmutableDispatchRuntime.ProcessMes
2021-05-26 09:36:34.7098 Results Service !!! Application End. !!!
 Project: User: Thread: 39
 Call stack: ExecutionContext.RunInternal => HttpRuntime.ReleaseResourcesAndUnloadAppDomain => HttpRuntime.Dispose => HttpApplicationFactory.Dispose => HttpApplicationFactory.FireApplicati
```

Listed: 3 Selected: 0 EMSSERVER_v1.E01/Partition 4 [952740MB]/EMS [NTFS]/[root]/VirtualDirectories/EMSApplicationServer/Log

Server Windows Defender Log Files Missing/Overwritten

Purpose: *These log files keep track of the activity of the built-in Anti-Virus software.*

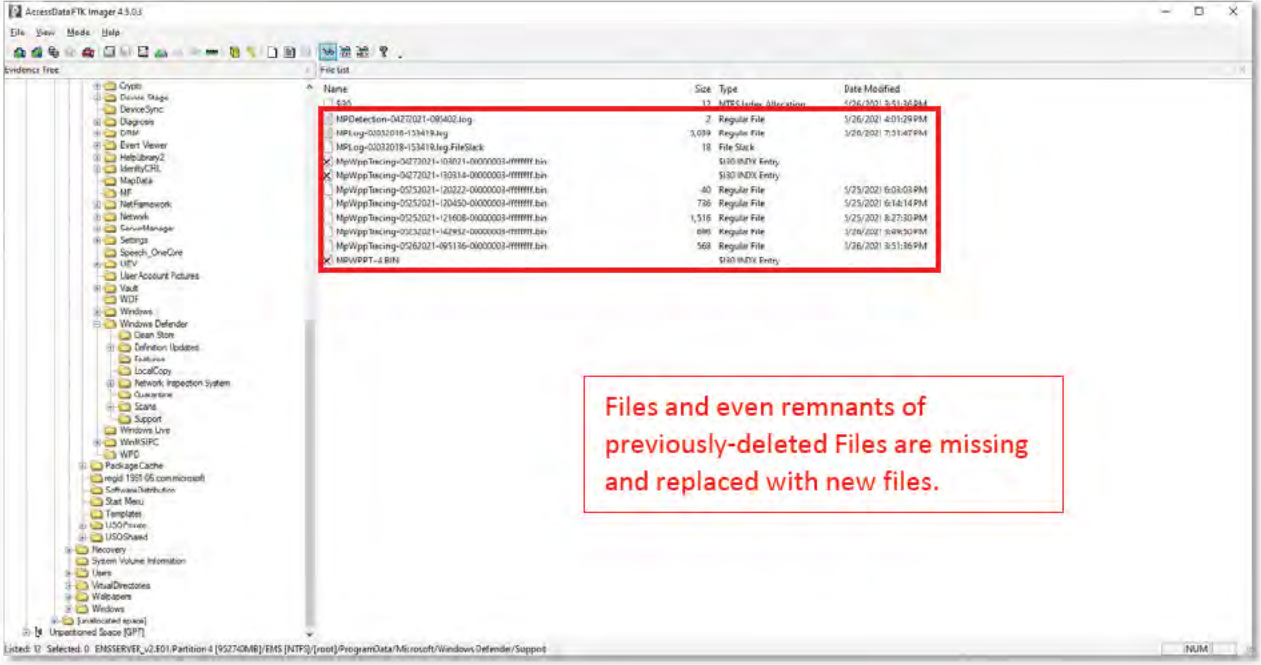
Figure 38 - EMS Server (5.11-CO) Windows Defender Log Files Before Dominion Update:



```
Name                                                   Size    Type                    Date Modified
MpWppTracing-06102019-131140-00000003-ffffffff.bin             $I30 INDX Entry
MPWPPT~4.BIN                                                   $I30 INDX Entry
MPLog-05072021-120450.log.FileSlack                      33    File Slack
MPLog-03082021-184449.log.FileSlack                       4    File Slack
$I30                                                     12    NTFS Index Allocation   3/7/2021 6:04:50 PM
MpWppTracing-03302021-092026-00000003-ffffffff.bin      160    Regular File            3/30/2021 3:25:41 PM
MpWppTracing-03182021-105340-00000003-ffffffff.bin      228    Regular File            3/18/2021 4:58:41 PM
MPDetection-03182021-105340.log                           1    Regular File            3/18/2021 5:10:26 PM
MpWppTracing-01052021-164513-00000003-ffffffff.bin    4,096    Regular File            3/18/2021 4:51:51 PM
MpWppTracing-03302021-093006-00000003-ffffffff.bin    4,096    Regular File            3/30/2021 3:30:05 PM
MPLog-05072021-120450.log                            16,224    Regular File            5/23/2021 10:03:51 PM
MPLog-03082021-184449.log                            32,773    Regular File            3/7/2021 4:04:51 PM
MpWppTracing-03182021-110015-00000003-ffffffff.bin    1,180    Regular File            3/30/2021 3:18:59 PM
MpWppTracing-06252019-105814-00000003-ffffffff.bin    4,096    Regular File            6/25/2019 5:18:03 PM
MpWppTracing-06252019-105548-00000003-ffffffff.bin       36    Regular File            6/25/2019 4:56:19 PM
MpWppTracing-06122019-150811-00000003-ffffffff.bin    2,036    Regular File            6/12/2019 9:24:41 PM
MpWppTracing-06112019-094415-00000003-ffffffff.bin      376    Regular File            6/11/2019 3:56:45 PM
MpWppTracing-06102019-100354-00000003-ffffffff.bin      112    Regular File            6/10/2019 5:09:20 PM
MPDetection-06102019-095254.log                           2    Regular File            6/26/2019 10:10:24 PM
MpWppTracing-06102019-133137-00000003-ffffffff.bin       48    Regular File            6/10/2019 7:33:14 PM
MpWppTracing-06102019-101810-00000003-ffffffff.bin      136    Regular File            6/10/2019 5:24:14 PM
MpWppTracing-06102019-102610-00000003-ffffffff.bin       72    Regular File            6/10/2019 5:27:32 PM
MpWppTracing-09032019-122548-00000003-ffffffff.bin    1,808    Regular File            9/4/2019 8:37:56 PM
MPDetection-09032019-122347.log                           1    Regular File            10/21/2019 5:18:35 PM
MPLog-09122016-043440.log                                 0    Regular File            12/14/2020 10:53:33 PM
```

Listed: 25 Selected: 0 EMSSERVER.E01/Partition 2 [952843MB]/OS [NTFS]/[root]/ProgramData/Microsoft/Windows Defender/Support

Figure 39 - EMS Server (5.13) Windows Defender Log Files After



```
Name                                                   Size    Type                    Date Modified
$I30                                                     12    NTFS Index Allocation   5/26/2021 3:51:36 PM
MPDetection-04272021-095402.log                           2    Regular File            5/26/2021 4:01:29 PM
MPLog-03032018-153419.log                             3,039    Regular File            5/26/2021 7:51:47 PM
MPLog-03032018-153419.log.FileSlack                      18    File Slack
MpWppTracing-04272021-103021-00000003-ffffffff.bin             $I30 INDX Entry
MpWppTracing-04272021-130314-00000003-ffffffff.bin             $I30 INDX Entry
MpWppTracing-05252021-120222-00000003-ffffffff.bin       40    Regular File            5/25/2021 6:03:03 PM
MpWppTracing-05252021-120450-00000003-ffffffff.bin      736    Regular File            5/25/2021 6:14:14 PM
MpWppTracing-05252021-121608-00000003-ffffffff.bin    1,516    Regular File            5/25/2021 8:27:30 PM
MpWppTracing-05252021-142952-00000003-ffffffff.bin      696    Regular File            5/26/2021 9:49:50 PM
MpWppTracing-05262021-095136-00000003-ffffffff.bin      568    Regular File            5/26/2021 3:51:36 PM
MPWPPT~4.BIN                                                   $I30 INDX Entry
```

Files and even remnants of previously-deleted Files are missing and replaced with new files.

Listed: 12 Selected: 0 EMSSERVER_v2.E01/Partition 4 [952740MB]/EMS [NTFS]/[root]/ProgramData/Microsoft/Windows Defender/Support

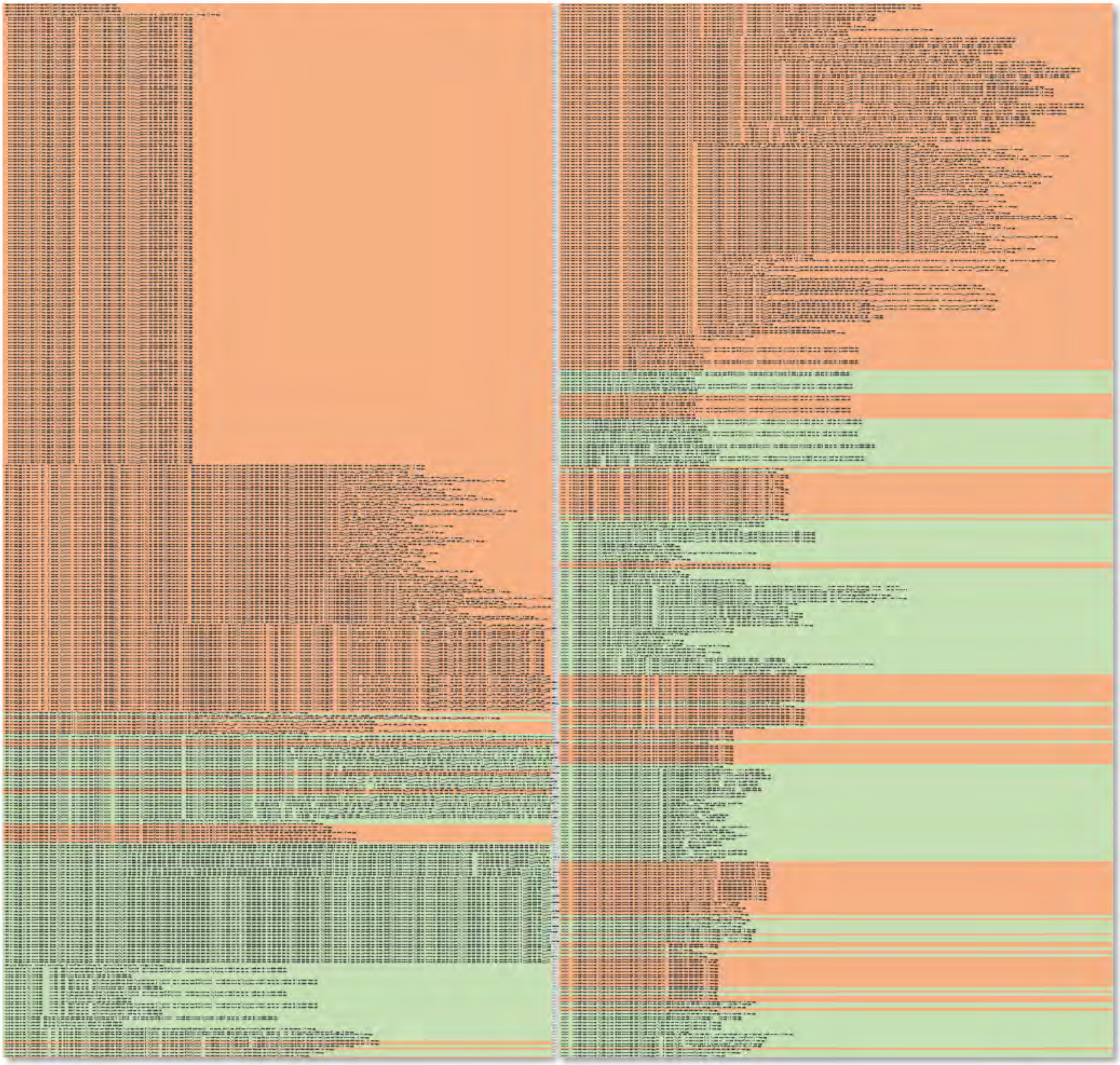
Server List of .log files in Before Image that were Deleted.

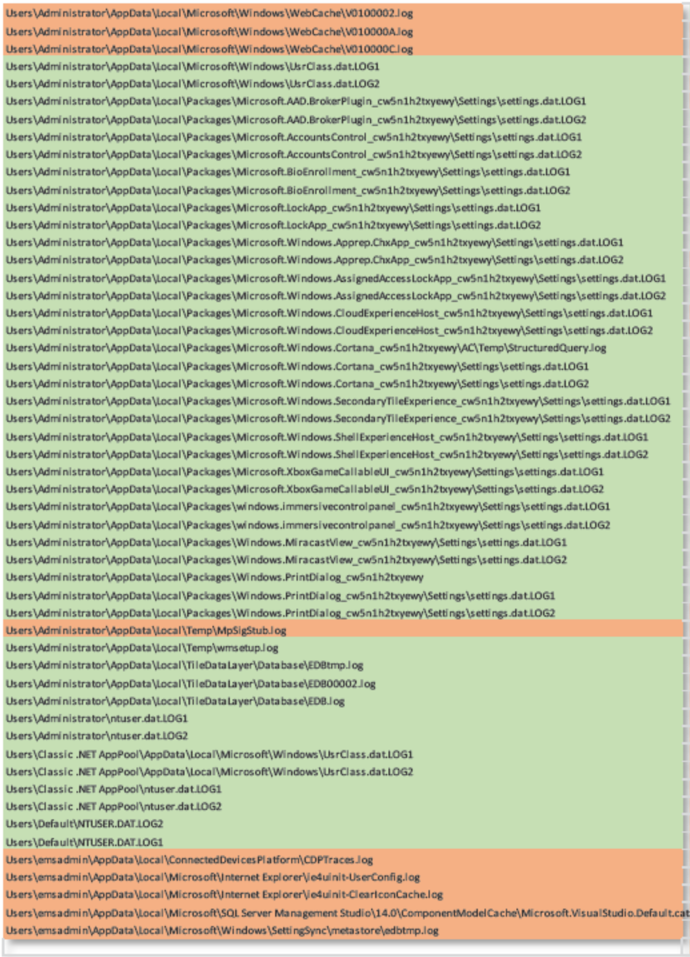
This list that follows this paragraph is a comparison of the Before and After forensic images of the Mesa County EMS Server. It is a comparative list of files that were deleted – either deliberately erased or overwritten with disregard for the preservation of these files, some of which contain ELECTION RELATED data.

Each line in the image below is the full path listing to each one of the 807 files that end with the word ".log" found on the EMS Server before the Dominion update was applied.

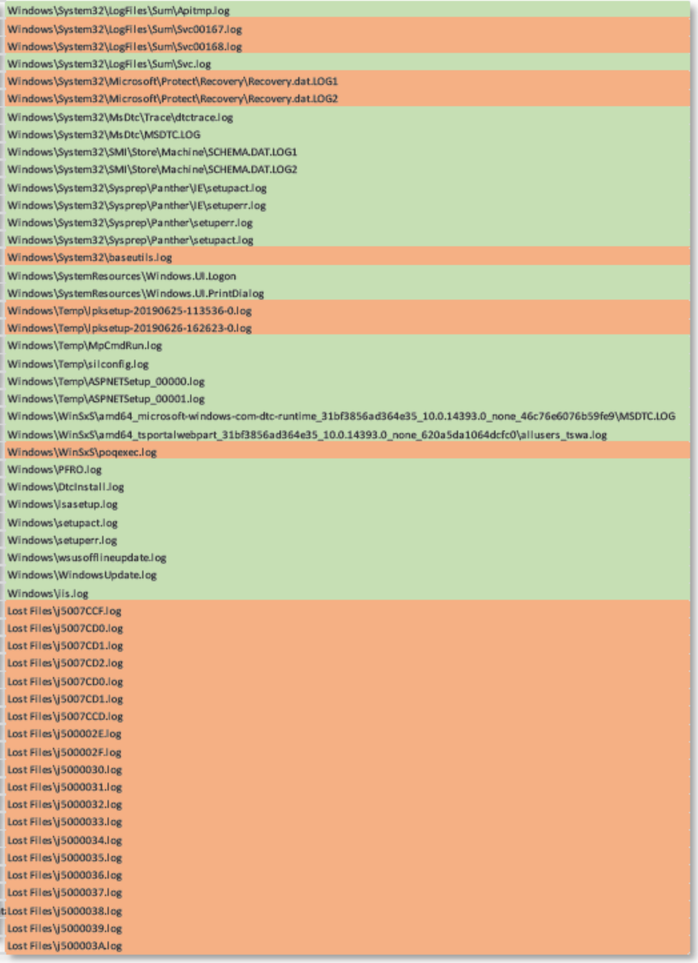
The Color code shows what happened to them After Dominion's update. Of all the files on the server Before the update – files highlighted in Green are still present on the server after the update, while files highlighted in light red have been overwritten and are deleted and not present in the image taken After the update.

Figure 40 - EMS Server Before/After .log File Comparison List





```
Users\Administrator\AppData\Local\Microsoft\Windows\WebCache\V0100002.log
Users\Administrator\AppData\Local\Microsoft\Windows\WebCache\V010000A.log
Users\Administrator\AppData\Local\Microsoft\Windows\WebCache\V010000C.log
Users\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
Users\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.AccountsControl_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Microsoft.AccountsControl_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.BioEnrollment_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Microsoft.BioEnrollment_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.LockApp_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Microsoft.LockApp_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.AssignedAccessLockApp_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.AssignedAccessLockApp_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\Temp\StructuredQuery.log
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.SecondaryTileExperience_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.SecondaryTileExperience_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.XboxGameCallableUI_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Microsoft.XboxGameCallableUI_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\windows.immersivecontrolpanel_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\windows.immersivecontrolpanel_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Windows.MiracastView_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Windows.MiracastView_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Windows.PrintDialog_cw5n1h2txyewy
Users\Administrator\AppData\Local\Packages\Windows.PrintDialog_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Windows.PrintDialog_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Temp\MpSigStub.log
Users\Administrator\AppData\Local\Temp\wmsetup.log
Users\Administrator\AppData\Local\TileDataLayer\Database\EDBtmp.log
Users\Administrator\AppData\Local\TileDataLayer\Database\EDB00002.log
Users\Administrator\AppData\Local\TileDataLayer\Database\EDB.log
Users\Administrator\ntuser.dat.LOG1
Users\Administrator\ntuser.dat.LOG2
Users\Classic .NET AppPool\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
Users\Classic .NET AppPool\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2
Users\Classic .NET AppPool\ntuser.dat.LOG1
Users\Classic .NET AppPool\ntuser.dat.LOG2
Users\Default\NTUSER.DAT.LOG2
Users\Default\NTUSER.DAT.LOG1
Users\emsadmin\AppData\Local\ConnectedDevicesPlatform\CDPTraces.log
Users\emsadmin\AppData\Local\Microsoft\Internet Explorer\ie4uinit-UserConfig.log
Users\emsadmin\AppData\Local\Microsoft\Internet Explorer\ie4uinit-ClearIconCache.log
Users\emsadmin\AppData\Local\Microsoft\SQL Server Management Studio\14.0\ComponentModelCache\Microsoft.VisualStudio.Default.cat
Users\emsadmin\AppData\Local\Microsoft\Windows\SettingSync\metastore\edbtmp.log
```



```
Windows\System32\LogFiles\Sum\Apitmp.log
Windows\System32\LogFiles\Sum\Svc00167.log
Windows\System32\LogFiles\Sum\Svc00168.log
Windows\System32\LogFiles\Sum\Svc.log
Windows\System32\Microsoft\Protect\Recovery\Recovery.dat.LOG1
Windows\System32\Microsoft\Protect\Recovery\Recovery.dat.LOG2
Windows\System32\MsDtc\Trace\dtctrace.log
Windows\System32\MsDtc\MSDTC.LOG
Windows\System32\SMI\Store\Machine\SCHEMA.DAT.LOG1
Windows\System32\SMI\Store\Machine\SCHEMA.DAT.LOG2
Windows\System32\Sysprep\Panther\IE\setupact.log
Windows\System32\Sysprep\Panther\IE\setuperr.log
Windows\System32\Sysprep\Panther\setuperr.log
Windows\System32\Sysprep\Panther\setupact.log
Windows\System32\baseutils.log
Windows\SystemResources\Windows.UI.Logon
Windows\SystemResources\Windows.UI.PrintDialog
Windows\Temp\lpksetup-20190625-113536-0.log
Windows\Temp\lpksetup-20190626-162623-0.log
Windows\Temp\MpCmdRun.log
Windows\Temp\silconfig.log
Windows\Temp\ASPNETSetup_00000.log
Windows\Temp\ASPNETSetup_00001.log
Windows\WinSxS\amd64_microsoft-windows-com-dtc-runtime_31bf3856ad364e35_10.0.14393.0_none_46c76e6076b59fe9\MSDTC.LOG
Windows\WinSxS\amd64_tsportalwebpart_31bf3856ad364e35_10.0.14393.0_none_620a5da1064dcfc0\allusers_tswa.log
Windows\WinSxS\poqexec.log
Windows\PFRO.log
Windows\DtcInstall.log
Windows\lsasetup.log
Windows\setupact.log
Windows\setuperr.log
Windows\wsusofflineupdate.log
Windows\WindowsUpdate.log
Windows\iis.log
Lost Files\j5007CCF.log
Lost Files\j5007CD0.log
Lost Files\j5007CD1.log
Lost Files\j5007CD2.log
Lost Files\j5007CD0.log
Lost Files\j5007CD1.log
Lost Files\j5007CCD.log
Lost Files\j500002E.log
Lost Files\j500002F.log
Lost Files\j5000030.log
Lost Files\j5000031.log
Lost Files\j5000032.log
Lost Files\j5000033.log
Lost Files\j5000034.log
Lost Files\j5000035.log
Lost Files\j5000036.log
Lost Files\j5000037.log
Lost Files\j5000038.log
Lost Files\j5000039.log
Lost Files\j500003A.log
```

Significant Number of Logfiles Missing

The dataset from which this spreadsheet was created was extracted from the EnCase images of the original evidence on the hard drives of the EMS Server and had a traceable chain of custody. While the images above are too small to be readable, the entire content of this list is reproduced in Appendix A.

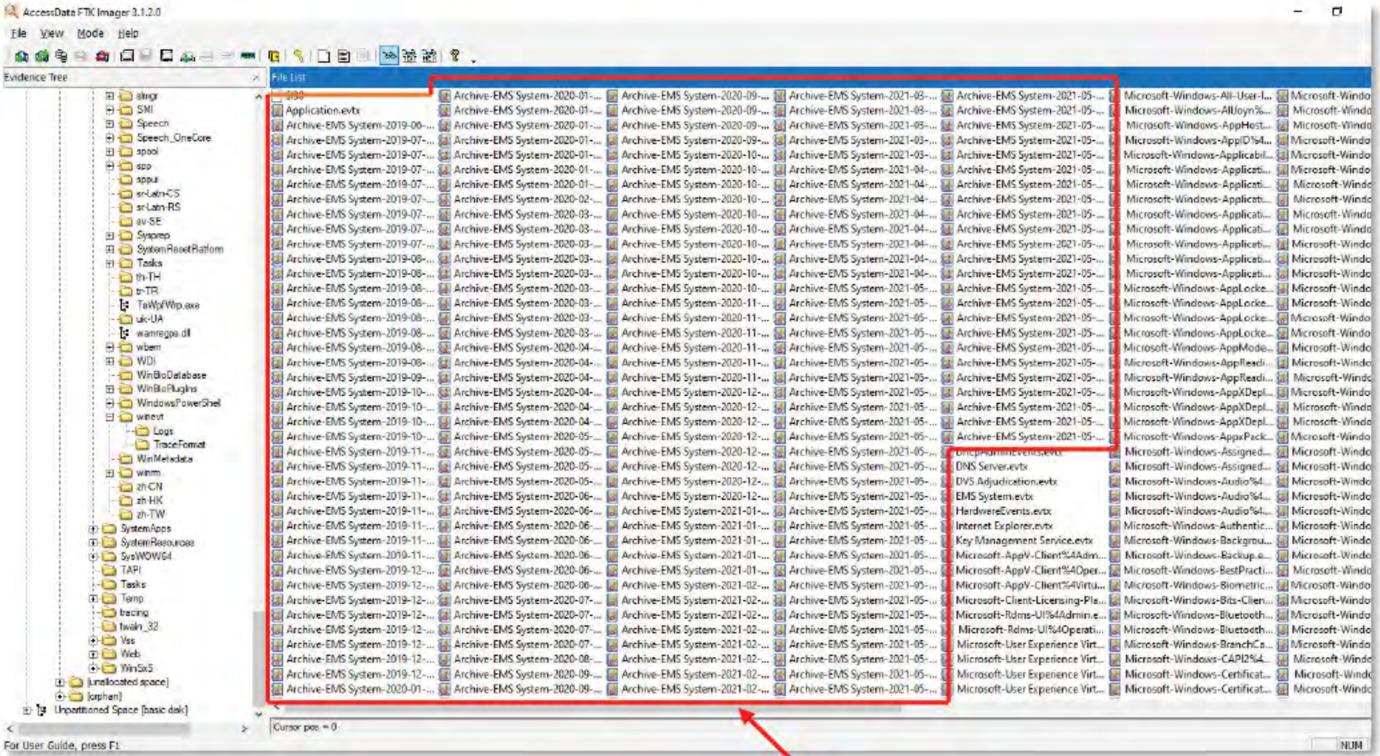
Of the original 807 ".log" files on the EMS Server before Dominion's update, only 302 remain, and 505 ".log" files have been deleted or overwritten.

Of the files *that remain*, the forensic examination has not yet verified whether the content of these files (which have the same filename and Path – e.g., in the same directories) is unchanged. The files that have been deleted DO include files that constitute Election Records and are subject to Federal and State data retention laws.

This list is only 807 files, and the text size is so small that the content is barely readable. The list of files has been broken down into small subsets because the number of files on the entire server totals 363,321 files, many of which are provided by Microsoft as part of the Windows Server 2016 operating system and its associated application programs and are not Election Related and do not contain actual Election Data.

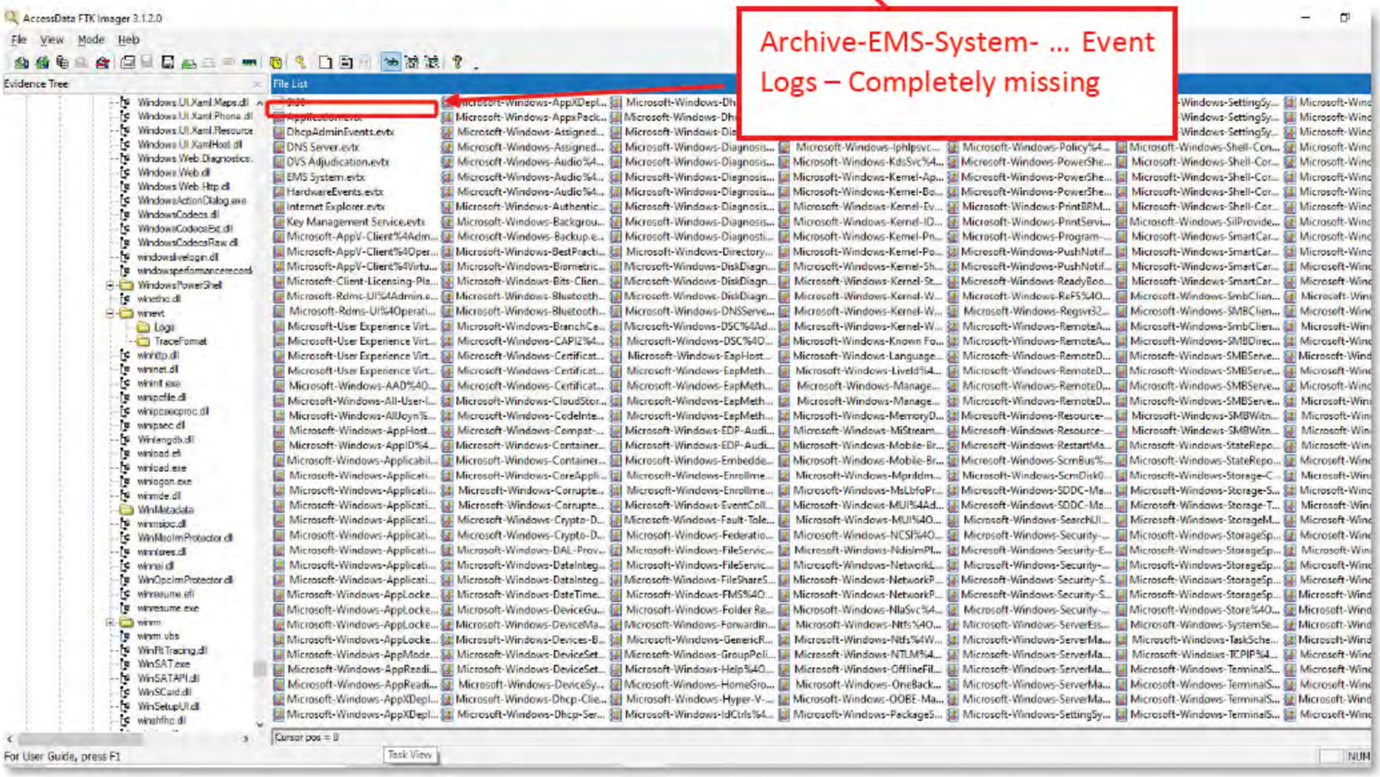
List of .evtx Event Log Files deleted

Figure 41 - EMS Server (5.11-CO) List of .evtx Event Log Files Before



```
$I30
Application.evtx
Archive-EMS System-2019-06-...
Archive-EMS System-2019-07-...
Archive-EMS System-2019-07-...
Archive-EMS System-2019-07-...
Archive-EMS System-2019-07-...
Archive-EMS System-2019-07-...
Archive-EMS System-2019-07-...
Archive-EMS System-2019-07-...
Archive-EMS System-2019-07-...
Archive-EMS System-2019-08-...
Archive-EMS System-2019-08-...
Archive-EMS System-2019-08-...
Archive-EMS System-2019-08-...
Archive-EMS System-2019-08-...
Archive-EMS System-2019-08-...
Archive-EMS System-2019-08-...
Archive-EMS System-2019-08-...
Archive-EMS System-2019-09-...
Archive-EMS System-2019-10-...
Archive-EMS System-2019-10-...
Archive-EMS System-2019-10-...
Archive-EMS System-2019-10-...
Archive-EMS System-2019-11-...
Archive-EMS System-2019-11-...
Archive-EMS System-2019-11-...
Archive-EMS System-2019-11-...
Archive-EMS System-2019-11-...
Archive-EMS System-2019-11-...
Archive-EMS System-2019-11-...
Archive-EMS System-2019-11-...
Archive-EMS System-2019-12-...
Archive-EMS System-2019-12-...
Archive-EMS System-2019-12-...
Archive-EMS System-2019-12-...
Archive-EMS System-2019-12-...
Archive-EMS System-2019-12-...
Archive-EMS System-2019-12-...
Archive-EMS System-2019-12-...
Archive-EMS System-2020-01-...

Archive-EMS System-2020-01-...
Archive-EMS System-2020-01-...
Archive-EMS System-2020-01-...
Archive-EMS System-2020-01-...
Archive-EMS System-2020-01-...
Archive-EMS System-2020-01-...
Archive-EMS System-2020-01-...
Archive-EMS System-2020-02-...
Archive-EMS System-2020-03-...
Archive-EMS System-2020-03-...
Archive-EMS System-2020-03-...
Archive-EMS System-2020-03-...
Archive-EMS System-2020-03-...
Archive-EMS System-2020-03-...
Archive-EMS System-2020-03-...
Archive-EMS System-2020-03-...
Archive-EMS System-2020-03-...
Archive-EMS System-2020-04-...
Archive-EMS System-2020-04-...
Archive-EMS System-2020-04-...
Archive-EMS System-2020-04-...
Archive-EMS System-2020-04-...
Archive-EMS System-2020-04-...
Archive-EMS System-2020-05-...
Archive-EMS System-2020-05-...
Archive-EMS System-2020-05-...
Archive-EMS System-2020-05-...
Archive-EMS System-2020-06-...
Archive-EMS System-2020-06-...
Archive-EMS System-2020-06-...
Archive-EMS System-2020-06-...
Archive-EMS System-2020-06-...
Archive-EMS System-2020-06-...
Archive-EMS System-2020-06-...
Archive-EMS System-2020-07-...
Archive-EMS System-2020-07-...
Archive-EMS System-2020-07-...
Archive-EMS System-2020-07-...
Archive-EMS System-2020-08-...
Archive-EMS System-2020-09-...
Archive-EMS System-2020-09-...

Archive-EMS System-2020-09-...
Archive-EMS System-2020-09-...
Archive-EMS System-2020-09-...
Archive-EMS System-2020-09-...
Archive-EMS System-2020-10-...
Archive-EMS System-2020-10-...
Archive-EMS System-2020-10-...
Archive-EMS System-2020-10-...
Archive-EMS System-2020-10-...
Archive-EMS System-2020-10-...
Archive-EMS System-2020-10-...
Archive-EMS System-2020-10-...
Archive-EMS System-2020-10-...
Archive-EMS System-2020-10-...
Archive-EMS System-2020-11-...
Archive-EMS System-2020-11-...
Archive-EMS System-2020-11-...
Archive-EMS System-2020-11-...
Archive-EMS System-2020-11-...
Archive-EMS System-2020-11-...
Archive-EMS System-2020-12-...
Archive-EMS System-2020-12-...
Archive-EMS System-2020-12-...
Archive-EMS System-2020-12-...
Archive-EMS System-2020-12-...
Archive-EMS System-2020-12-...
Archive-EMS System-2020-12-...
Archive-EMS System-2020-12-...
Archive-EMS System-2021-01-...
Archive-EMS System-2021-01-...
Archive-EMS System-2021-01-...
Archive-EMS System-2021-01-...
Archive-EMS System-2021-01-...
Archive-EMS System-2021-02-...
Archive-EMS System-2021-02-...
Archive-EMS System-2021-02-...
Archive-EMS System-2021-02-...
Archive-EMS System-2021-02-...
Archive-EMS System-2021-02-...
Archive-EMS System-2021-02-...
Archive-EMS System-2021-02-...

Archive-EMS System-2021-03-...
Archive-EMS System-2021-03-...
Archive-EMS System-2021-03-...
Archive-EMS System-2021-03-...
Archive-EMS System-2021-03-...
Archive-EMS System-2021-04-...
Archive-EMS System-2021-04-...
Archive-EMS System-2021-04-...
Archive-EMS System-2021-04-...
Archive-EMS System-2021-04-...
Archive-EMS System-2021-04-...
Archive-EMS System-2021-04-...
Archive-EMS System-2021-04-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...

Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
Archive-EMS System-2021-05-...
DhcpAdminEvents.evtx
DNS Server.evtx
DVS Adjudication.evtx
EMS System.evtx
HardwareEvents.evtx
Internet Explorer.evtx
Key Management Service.evtx
Microsoft-AppV-Client%4Adm...
Microsoft-AppV-Client%4Oper...
Microsoft-AppV-Client%4Virtu...
Microsoft-Client-Licensing-Pla...
Microsoft-Rdms-UI%4Admin.e...
Microsoft-Rdms-UI%4Operati...
Microsoft-User Experience Virt...
Microsoft-User Experience Virt...
Microsoft-User Experience Virt...
Microsoft-User Experience Virt...

Microsoft-Windows-All-User-I...
Microsoft-Windows-AllJoyn%...
Microsoft-Windows-AppHost...
Microsoft-Windows-AppID%4...
Microsoft-Windows-Applicabil...
Microsoft-Windows-Applicati...
Microsoft-Windows-Applicati...
Microsoft-Windows-Applicati...
Microsoft-Windows-Applicati...
Microsoft-Windows-Applicati...
Microsoft-Windows-Applicati...
Microsoft-Windows-Applicati...
Microsoft-Windows-Applicati...
Microsoft-Windows-AppLocke...
Microsoft-Windows-AppLocke...
Microsoft-Windows-AppLocke...
Microsoft-Windows-AppLocke...
Microsoft-Windows-AppMode...
Microsoft-Windows-AppReadi...
Microsoft-Windows-AppReadi...
Microsoft-Windows-AppXDepl...
Microsoft-Windows-AppXDepl...
Microsoft-Windows-AppXDepl...
Microsoft-Windows-AppxPack...
Microsoft-Windows-Assigned...
Microsoft-Windows-Assigned...
Microsoft-Windows-Audio%4...
Microsoft-Windows-Audio%4...
Microsoft-Windows-Audio%4...
Microsoft-Windows-Authentic...
Microsoft-Windows-Backgrou...
Microsoft-Windows-Backup.e...
Microsoft-Windows-BestPracti...
Microsoft-Windows-Biometric...
Microsoft-Windows-Bits-Clien...
Microsoft-Windows-Bluetooth...
Microsoft-Windows-Bluetooth...
Microsoft-Windows-BranchCa...
Microsoft-Windows-CAPI2%4...
Microsoft-Windows-Certificat...
Microsoft-Windows-Certificat...

Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
Microsoft-Windo
```

Figure 42 - EMS Server (5.13) List of .evtx Event Log Files After

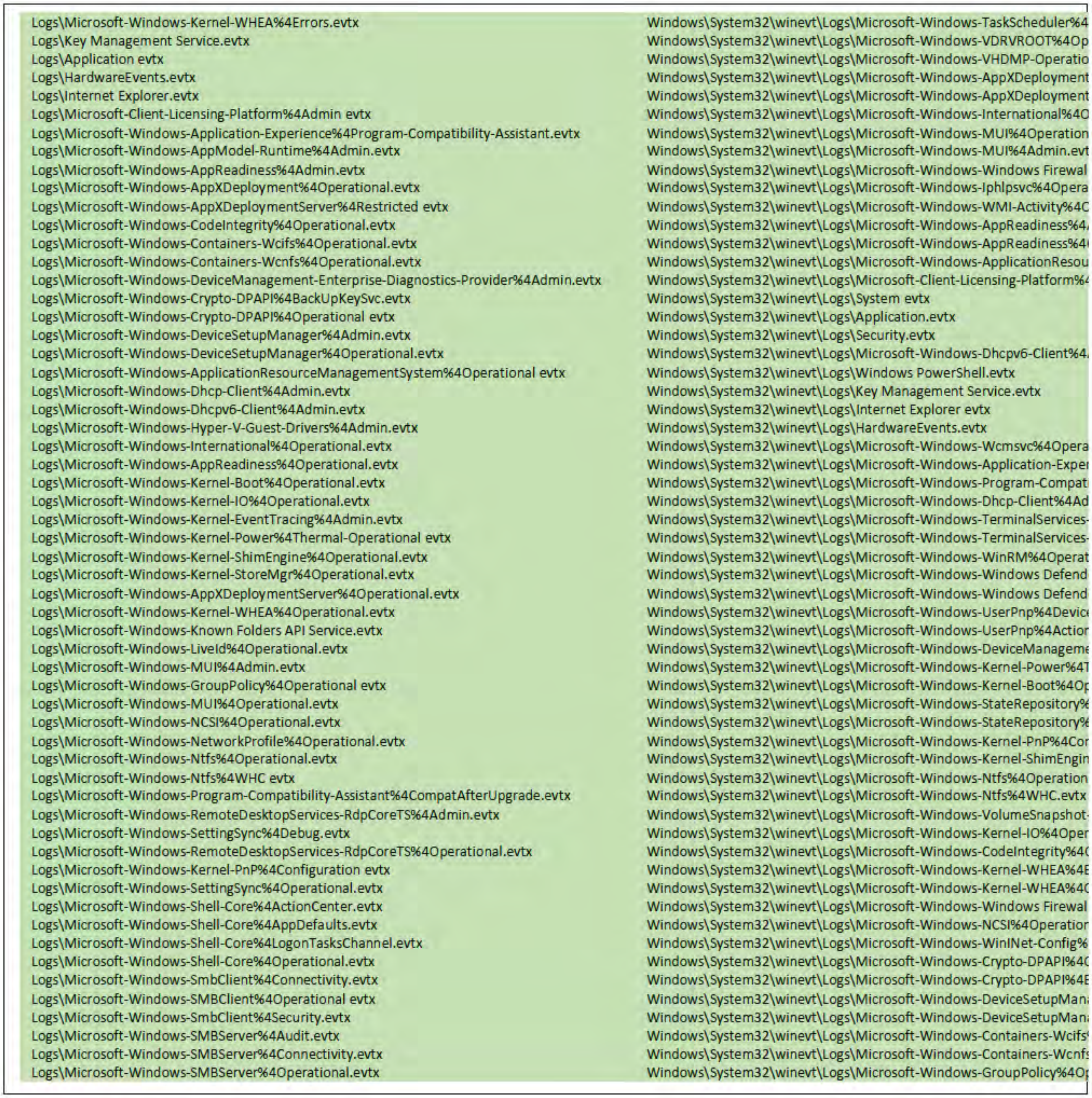


```
$I30
Application.evtx
DhcpAdminEvents.evtx
DNS Server.evtx
DVS Adjudication.evtx
EMS System.evtx
HardwareEvents.evtx
Internet Explorer.evtx
Key Management Service.evtx
Microsoft-AppV-Client%4Adm...
Microsoft-AppV-Client%4Oper...
Microsoft-AppV-Client%4Virtu...
Microsoft-Client-Licensing-Pla...
Microsoft-Rdms-UI%4Admin.e...
Microsoft-Rdms-UI%4Operati...
Microsoft-User Experience Virt...
Microsoft-User Experience Virt...
Microsoft-User Experience Virt...
Microsoft-User Experience Virt...
Microsoft-Windows-AAD%40...
Microsoft-Windows-All-User-I...
Microsoft-Windows-AllJoyn%...
Microsoft-Windows-AppHost...
Microsoft-Windows-AppID%4...
Microsoft-Windows-Applicabil...
Microsoft-Windows-Applicati...
Microsoft-Windows-Applicati...
Microsoft-Windows-Applicati...
Microsoft-Windows-Applicati...
Microsoft-Windows-Applicati...
Microsoft-Windows-Applicati...
Microsoft-Windows-Applicati...
Microsoft-Windows-Applicati...
Microsoft-Windows-AppLocke...
Microsoft-Windows-AppLocke...
Microsoft-Windows-AppLocke...
Microsoft-Windows-AppLocke...
Microsoft-Windows-AppMode...
Microsoft-Windows-AppReadi...
Microsoft-Windows-AppReadi...
Microsoft-Windows-AppXDepl...
Microsoft-Windows-AppXDepl...

Microsoft-Windows-AppXDepl...
Microsoft-Windows-AppxPack...
Microsoft-Windows-Assigned...
Microsoft-Windows-Assigned...
Microsoft-Windows-Audio%4...
Microsoft-Windows-Audio%4...
Microsoft-Windows-Audio%4...
Microsoft-Windows-Authentic...
Microsoft-Windows-Backgrou...
Microsoft-Windows-Backup.e...
Microsoft-Windows-BestPracti...
Microsoft-Windows-Biometric...
Microsoft-Windows-Bits-Clien...
Microsoft-Windows-Bluetooth...
Microsoft-Windows-Bluetooth...
Microsoft-Windows-BranchCa...
Microsoft-Windows-CAPI2%4...
Microsoft-Windows-Certificat...
Microsoft-Windows-Certificat...
Microsoft-Windows-Certificat...
Microsoft-Windows-CloudStor...
Microsoft-Windows-CodeInte...
Microsoft-Windows-Compat-...
Microsoft-Windows-Container...
Microsoft-Windows-Container...
Microsoft-Windows-CoreAppli...
Microsoft-Windows-Corrupte...
Microsoft-Windows-Corrupte...
Microsoft-Windows-Crypto-D...
Microsoft-Windows-Crypto-D...
Microsoft-Windows-DAL-Prov...
Microsoft-Windows-DataInteg...
Microsoft-Windows-DataInteg...
Microsoft-Windows-DateTime...
Microsoft-Windows-DeviceGu...
Microsoft-Windows-DeviceMa...
Microsoft-Windows-Devices-B...
Microsoft-Windows-DeviceSet...
Microsoft-Windows-DeviceSet...
Microsoft-Windows-DeviceSy...
Microsoft-Windows-Dhcp-Clie...
Microsoft-Windows-Dhcp-Ser...

Microsoft-Windows-Dh
Microsoft-Windows-Dh
Microsoft-Windows-Dia
Microsoft-Windows-Diagnosis...
Microsoft-Windows-Diagnosis...
Microsoft-Windows-Diagnosis...
Microsoft-Windows-Diagnosis...
Microsoft-Windows-Diagnosis...
Microsoft-Windows-Diagnosis...
Microsoft-Windows-Diagnosti...
Microsoft-Windows-Directory...
Microsoft-Windows-DiskDiagn...
Microsoft-Windows-DiskDiagn...
Microsoft-Windows-DiskDiagn...
Microsoft-Windows-DNSServe...
Microsoft-Windows-DSC%4Ad...
Microsoft-Windows-DSC%4O...
Microsoft-Windows-EapHost...
Microsoft-Windows-EapMeth...
Microsoft-Windows-EapMeth...
Microsoft-Windows-EapMeth...
Microsoft-Windows-EapMeth...
Microsoft-Windows-EDP-Audi...
Microsoft-Windows-EDP-Audi...
Microsoft-Windows-Embedde...
Microsoft-Windows-Enrollme...
Microsoft-Windows-Enrollme...
Microsoft-Windows-EventColl...
Microsoft-Windows-Fault-Tole...
Microsoft-Windows-Federatio...
Microsoft-Windows-FileServic...
Microsoft-Windows-FileServic...
Microsoft-Windows-FileShareS...
Microsoft-Windows-FMS%4O...
Microsoft-Windows-Folder Re...
Microsoft-Windows-Forwardin...
Microsoft-Windows-GenericR...
Microsoft-Windows-GroupPoli...
Microsoft-Windows-Help%4O...
Microsoft-Windows-HomeGro...
Microsoft-Windows-Hyper-V-...
Microsoft-Windows-IdCtrls%4...

Microsoft-Windows-Iphlpsvc...
Microsoft-Windows-KdsSvc%4...
Microsoft-Windows-Kernel-Ap...
Microsoft-Windows-Kernel-Bo...
Microsoft-Windows-Kernel-Ev...
Microsoft-Windows-Kernel-IO...
Microsoft-Windows-Kernel-Pn...
Microsoft-Windows-Kernel-Po...
Microsoft-Windows-Kernel-Sh...
Microsoft-Windows-Kernel-St...
Microsoft-Windows-Kernel-W...
Microsoft-Windows-Kernel-W...
Microsoft-Windows-Kernel-W...
Microsoft-Windows-Known Fo...
Microsoft-Windows-Language...
Microsoft-Windows-LiveId%4...
Microsoft-Windows-Manage...
Microsoft-Windows-Manage...
Microsoft-Windows-MemoryD...
Microsoft-Windows-MiStream...
Microsoft-Windows-Mobile-Br...
Microsoft-Windows-Mobile-Br...
Microsoft-Windows-Mprddm...
Microsoft-Windows-MsLbfoPr...
Microsoft-Windows-MUI%4Ad...
Microsoft-Windows-MUI%4O...
Microsoft-Windows-NCSI%4O...
Microsoft-Windows-NdisImPl...
Microsoft-Windows-NetworkL...
Microsoft-Windows-NetworkP...
Microsoft-Windows-NetworkP...
Microsoft-Windows-NlaSvc%4...
Microsoft-Windows-Ntfs%4O...
Microsoft-Windows-Ntfs%4W...
Microsoft-Windows-NTLM%4...
Microsoft-Windows-OfflineFil...
Microsoft-Windows-OneBack...
Microsoft-Windows-OOBE-Ma...
Microsoft-Windows-PackageS...

Microsoft-Windows-Policy%4...
Microsoft-Windows-PowerShe...
Microsoft-Windows-PowerShe...
Microsoft-Windows-PowerShe...
Microsoft-Windows-PrintBRM...
Microsoft-Windows-PrintServi...
Microsoft-Windows-Program-...
Microsoft-Windows-PushNotif...
Microsoft-Windows-PushNotif...
Microsoft-Windows-ReadyBoo...
Microsoft-Windows-ReFS%4O...
Microsoft-Windows-Regsvr32...
Microsoft-Windows-RemoteA...
Microsoft-Windows-RemoteA...
Microsoft-Windows-RemoteD...
Microsoft-Windows-RemoteD...
Microsoft-Windows-RemoteD...
Microsoft-Windows-RemoteD...
Microsoft-Windows-Resource-...
Microsoft-Windows-Resource-...
Microsoft-Windows-RestartMa...
Microsoft-Windows-ScmBus%...
Microsoft-Windows-ScmDisk0...
Microsoft-Windows-SDDC-Ma...
Microsoft-Windows-SDDC-Ma...
Microsoft-Windows-SearchUI...
Microsoft-Windows-Security-...
Microsoft-Windows-Security-E...
Microsoft-Windows-Security-...
Microsoft-Windows-Security-S...
Microsoft-Windows-Security-S...
Microsoft-Windows-Security-...
Microsoft-Windows-ServerEss...
Microsoft-Windows-ServerMa...
Microsoft-Windows-ServerMa...
Microsoft-Windows-ServerMa...
Microsoft-Windows-ServerMa...
Microsoft-Windows-ServerMa...
Microsoft-Windows-SettingSy...

-Windows-SettingSy...
-Windows-SettingSy...
-Windows-SettingSy...
Microsoft-Windows-Shell-Con...
Microsoft-Windows-Shell-Cor...
Microsoft-Windows-Shell-Cor...
Microsoft-Windows-Shell-Cor...
Microsoft-Windows-Shell-Cor...
Microsoft-Windows-SilProvide...
Microsoft-Windows-SmartCar...
Microsoft-Windows-SmartCar...
Microsoft-Windows-SmartCar...
Microsoft-Windows-SmartCar...
Microsoft-Windows-SmbClien...
Microsoft-Windows-SMBClien...
Microsoft-Windows-SmbClien...
Microsoft-Windows-SMBDirec...
Microsoft-Windows-SMBServe...
Microsoft-Windows-SMBServe...
Microsoft-Windows-SMBServe...
Microsoft-Windows-SMBServe...
Microsoft-Windows-SMBWitn...
Microsoft-Windows-SMBWitn...
Microsoft-Windows-StateRepo...
Microsoft-Windows-StateRepo...
Microsoft-Windows-Storage-C...
Microsoft-Windows-Storage-S...
Microsoft-Windows-Storage-T...
Microsoft-Windows-StorageM...
Microsoft-Windows-StorageSp...
Microsoft-Windows-StorageSp...
Microsoft-Windows-StorageSp...
Microsoft-Windows-StorageSp...
Microsoft-Windows-StorageSp...
Microsoft-Windows-Store%4O...
Microsoft-Windows-SystemSe...
Microsoft-Windows-TaskSche...
Microsoft-Windows-TCPIP%4...
Microsoft-Windows-TerminalS...
Microsoft-Windows-TerminalS...
Microsoft-Windows-TerminalS...
Microsoft-Windows-TerminalS...

Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
Microsoft-Wind
```

This list that follows this paragraph is a comparison of the Before and After forensic images of the Mesa County EMS Server. It is a comparative list of files that were deleted – either deliberately erased or overwritten with disregard for the preservation of these files, some of which contain ELECTION RELATED data. A readable list is in Appendix C.

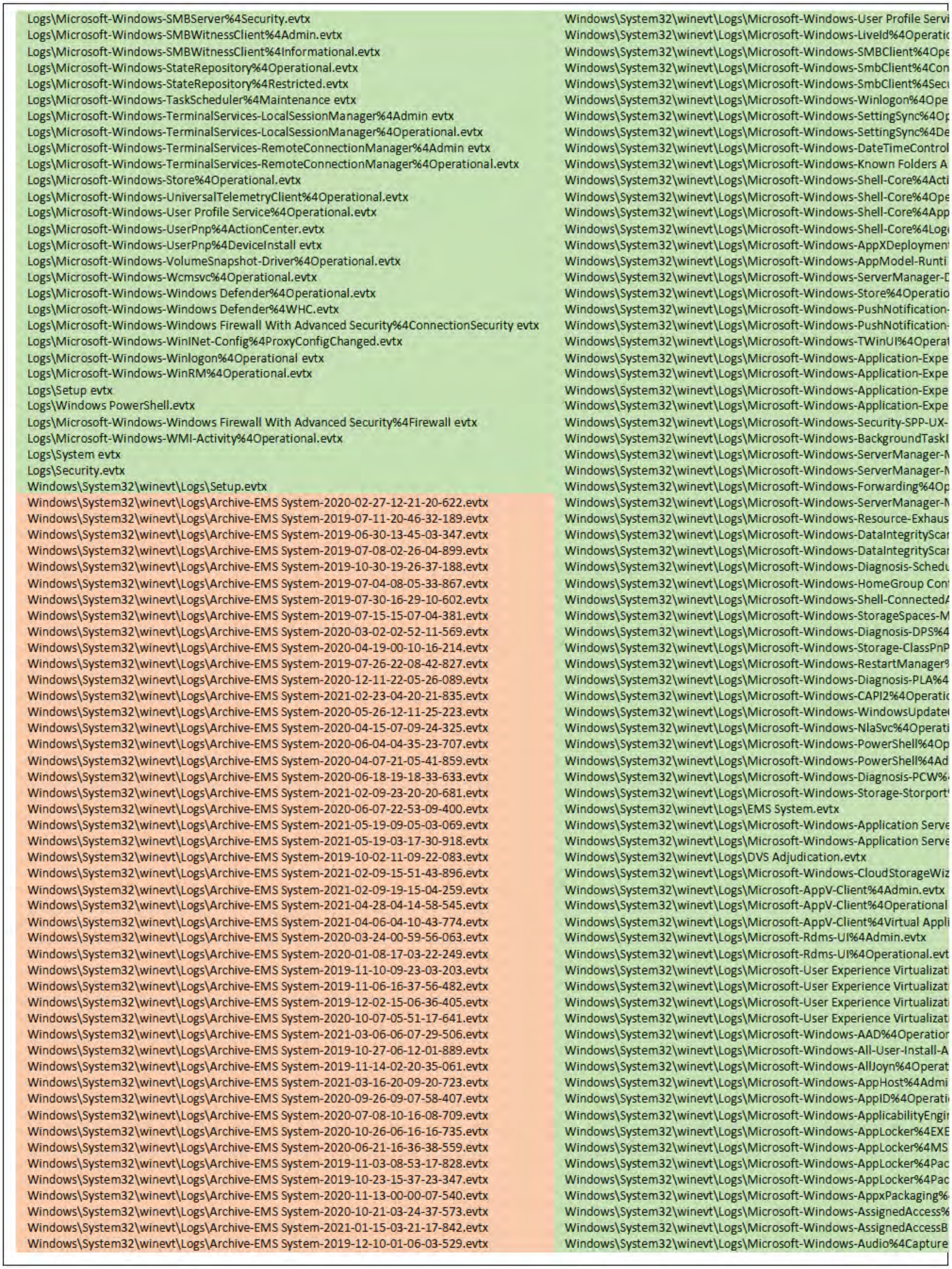
Each line in the image below is the full path listing (e.g., comparision of file names, not content) to each one of the 580 files that end with the word ".evtx" found on the EMS Server before the Dominion update was applied. 190 Event Log Files were deleted.

The Color code shows their status After Dominion's update. Of all the files on the server Before the update – files highlighted in Green are still present (although possibly changed) on the server after the update, while files highlighted in light red have been overwritten and are deleted and not present in the image After the update.



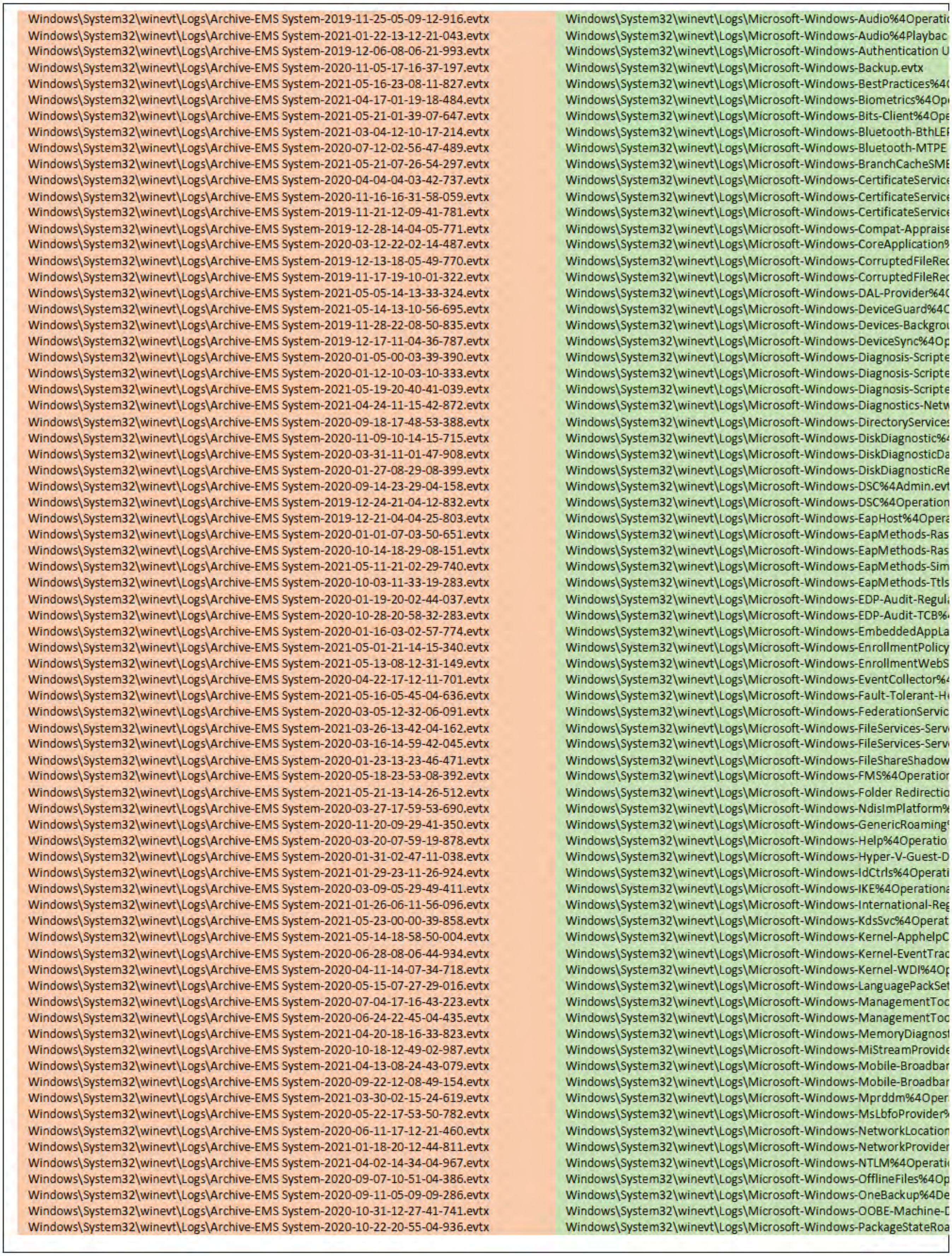
```
Logs\Microsoft-Windows-Kernel-WHEA%4Errors.evtx
Logs\Key Management Service.evtx
Logs\Application evtx
Logs\HardwareEvents.evtx
Logs\Internet Explorer.evtx
Logs\Microsoft-Client-Licensing-Platform%4Admin evtx
Logs\Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx
Logs\Microsoft-Windows-AppModel-Runtime%4Admin.evtx
Logs\Microsoft-Windows-AppReadiness%4Admin.evtx
Logs\Microsoft-Windows-AppXDeployment%4Operational.evtx
Logs\Microsoft-Windows-AppXDeploymentServer%4Restricted evtx
Logs\Microsoft-Windows-CodeIntegrity%4Operational.evtx
Logs\Microsoft-Windows-Containers-Wcifs%4Operational.evtx
Logs\Microsoft-Windows-Containers-Wcnfs%4Operational.evtx
Logs\Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider%4Admin.evtx
Logs\Microsoft-Windows-Crypto-DPAPI%4BackUpKeySvc.evtx
Logs\Microsoft-Windows-Crypto-DPAPI%4Operational evtx
Logs\Microsoft-Windows-DeviceSetupManager%4Admin.evtx
Logs\Microsoft-Windows-DeviceSetupManager%4Operational.evtx
Logs\Microsoft-Windows-ApplicationResourceManagementSystem%4Operational evtx
Logs\Microsoft-Windows-Dhcp-Client%4Admin.evtx
Logs\Microsoft-Windows-Dhcpv6-Client%4Admin.evtx
Logs\Microsoft-Windows-Hyper-V-Guest-Drivers%4Admin.evtx
Logs\Microsoft-Windows-International%4Operational.evtx
Logs\Microsoft-Windows-AppReadiness%4Operational.evtx
Logs\Microsoft-Windows-Kernel-Boot%4Operational.evtx
Logs\Microsoft-Windows-Kernel-IO%4Operational.evtx
Logs\Microsoft-Windows-Kernel-EventTracing%4Admin.evtx
Logs\Microsoft-Windows-Kernel-Power%4Thermal-Operational evtx
Logs\Microsoft-Windows-Kernel-ShimEngine%4Operational.evtx
Logs\Microsoft-Windows-Kernel-StoreMgr%4Operational.evtx
Logs\Microsoft-Windows-AppXDeploymentServer%4Operational.evtx
Logs\Microsoft-Windows-Kernel-WHEA%4Operational.evtx
Logs\Microsoft-Windows-Known Folders API Service.evtx
Logs\Microsoft-Windows-LiveId%4Operational.evtx
Logs\Microsoft-Windows-MUI%4Admin.evtx
Logs\Microsoft-Windows-GroupPolicy%4Operational evtx
Logs\Microsoft-Windows-MUI%4Operational.evtx
Logs\Microsoft-Windows-NCSI%4Operational.evtx
Logs\Microsoft-Windows-NetworkProfile%4Operational.evtx
Logs\Microsoft-Windows-Ntfs%4Operational.evtx
Logs\Microsoft-Windows-Ntfs%4WHC evtx
Logs\Microsoft-Windows-Program-Compatibility-Assistant%4CompatAfterUpgrade.evtx
Logs\Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Admin.evtx
Logs\Microsoft-Windows-SettingSync%4Debug.evtx
Logs\Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational.evtx
Logs\Microsoft-Windows-Kernel-PnP%4Configuration evtx
Logs\Microsoft-Windows-SettingSync%4Operational.evtx
Logs\Microsoft-Windows-Shell-Core%4ActionCenter.evtx
Logs\Microsoft-Windows-Shell-Core%4AppDefaults.evtx
Logs\Microsoft-Windows-Shell-Core%4LogonTasksChannel.evtx
Logs\Microsoft-Windows-Shell-Core%4Operational.evtx
Logs\Microsoft-Windows-SmbClient%4Connectivity.evtx
Logs\Microsoft-Windows-SMBClient%4Operational evtx
Logs\Microsoft-Windows-SmbClient%4Security.evtx
Logs\Microsoft-Windows-SMBServer%4Audit.evtx
Logs\Microsoft-Windows-SMBServer%4Connectivity.evtx
Logs\Microsoft-Windows-SMBServer%4Operational.evtx
```

```
Windows\System32\winevt\Logs\Microsoft-Windows-TaskScheduler%4
Windows\System32\winevt\Logs\Microsoft-Windows-VDRVROOT%4Op
Windows\System32\winevt\Logs\Microsoft-Windows-VHDMP-Operatio
Windows\System32\winevt\Logs\Microsoft-Windows-AppXDeployment
Windows\System32\winevt\Logs\Microsoft-Windows-AppXDeployment
Windows\System32\winevt\Logs\Microsoft-Windows-International%4O
Windows\System32\winevt\Logs\Microsoft-Windows-MUI%4Operation
Windows\System32\winevt\Logs\Microsoft-Windows-MUI%4Admin.evt
Windows\System32\winevt\Logs\Microsoft-Windows-Windows Firewal
Windows\System32\winevt\Logs\Microsoft-Windows-Iphlpsvc%4Opera
Windows\System32\winevt\Logs\Microsoft-Windows-WMI-Activity%4C
Windows\System32\winevt\Logs\Microsoft-Windows-AppReadiness%4
Windows\System32\winevt\Logs\Microsoft-Windows-AppReadiness%4
Windows\System32\winevt\Logs\Microsoft-Windows-ApplicationResou
Windows\System32\winevt\Logs\Microsoft-Client-Licensing-Platform%
Windows\System32\winevt\Logs\System evtx
Windows\System32\winevt\Logs\Application.evtx
Windows\System32\winevt\Logs\Security.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Dhcpv6-Client%4
Windows\System32\winevt\Logs\Windows PowerShell.evtx
Windows\System32\winevt\Logs\Key Management Service.evtx
Windows\System32\winevt\Logs\Internet Explorer evtx
Windows\System32\winevt\Logs\HardwareEvents.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Wcmsvc%4Opera
Windows\System32\winevt\Logs\Microsoft-Windows-Application-Exper
Windows\System32\winevt\Logs\Microsoft-Windows-Program-Compat
Windows\System32\winevt\Logs\Microsoft-Windows-Dhcp-Client%4Ad
Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-
Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-
Windows\System32\winevt\Logs\Microsoft-Windows-WinRM%4Operat
Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defend
Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defend
Windows\System32\winevt\Logs\Microsoft-Windows-UserPnp%4Device
Windows\System32\winevt\Logs\Microsoft-Windows-UserPnp%4Action
Windows\System32\winevt\Logs\Microsoft-Windows-DeviceManageme
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-Power%4T
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-Boot%4Op
Windows\System32\winevt\Logs\Microsoft-Windows-StateRepository%
Windows\System32\winevt\Logs\Microsoft-Windows-StateRepository%
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-PnP%4Con
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-ShimEngin
Windows\System32\winevt\Logs\Microsoft-Windows-Ntfs%4Operation
Windows\System32\winevt\Logs\Microsoft-Windows-Ntfs%4WHC.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-VolumeSnapshot-
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-IO%4Oper
Windows\System32\winevt\Logs\Microsoft-Windows-CodeIntegrity%4
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-WHEA%4E
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-WHEA%4O
Windows\System32\winevt\Logs\Microsoft-Windows-Windows Firewal
Windows\System32\winevt\Logs\Microsoft-Windows-NCSI%4Operation
Windows\System32\winevt\Logs\Microsoft-Windows-WinINet-Config%
Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-DPAPI%4O
Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-DPAPI%4B
Windows\System32\winevt\Logs\Microsoft-Windows-DeviceSetupMana
Windows\System32\winevt\Logs\Microsoft-Windows-DeviceSetupMana
Windows\System32\winevt\Logs\Microsoft-Windows-Containers-Wcifs
Windows\System32\winevt\Logs\Microsoft-Windows-Containers-Wcnfs
Windows\System32\winevt\Logs\Microsoft-Windows-GroupPolicy%4Op
```

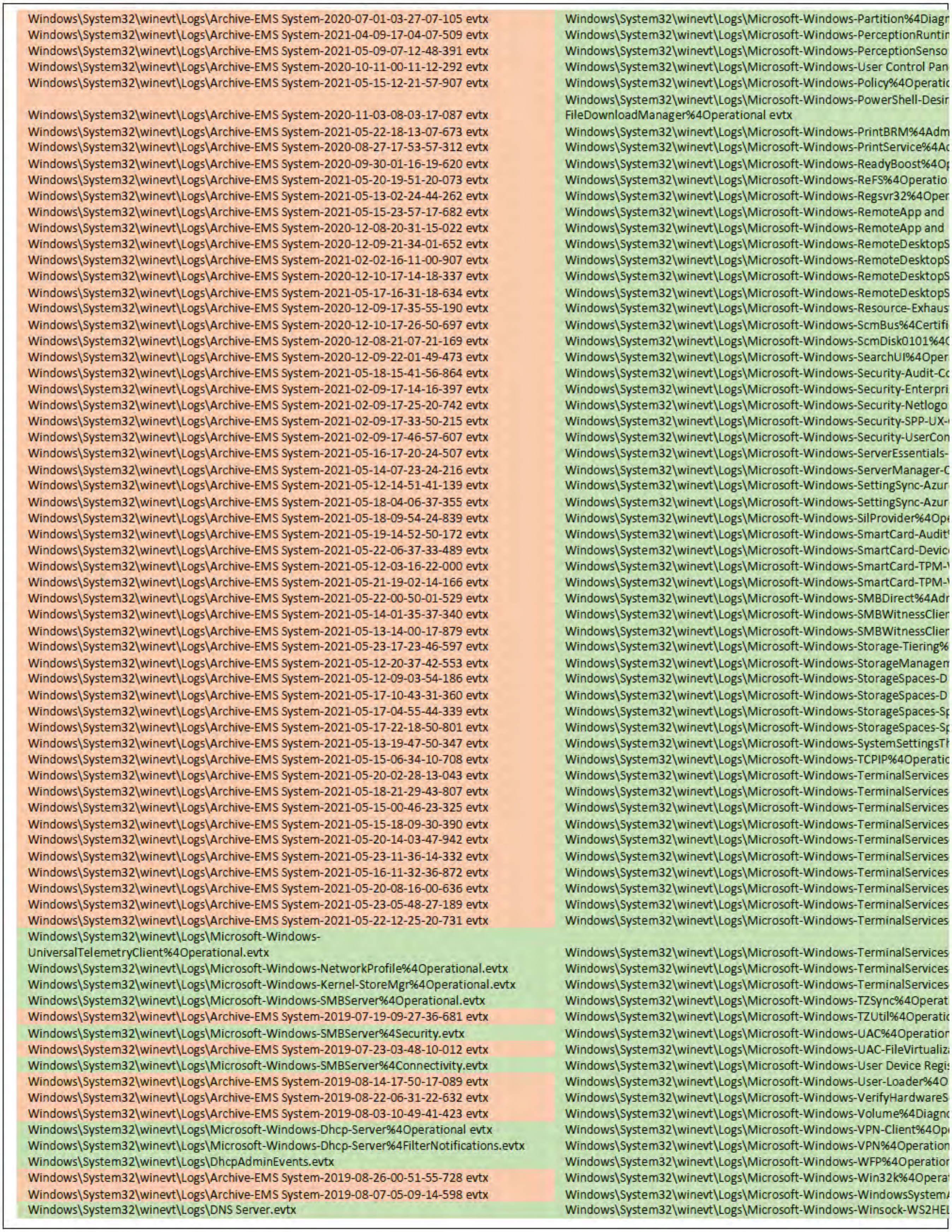


```
Logs\Microsoft-Windows-SMBServer%4Security.evtx
Logs\Microsoft-Windows-SMBWitnessClient%4Admin.evtx
Logs\Microsoft-Windows-SMBWitnessClient%4Informational.evtx
Logs\Microsoft-Windows-StateRepository%4Operational.evtx
Logs\Microsoft-Windows-StateRepository%4Restricted.evtx
Logs\Microsoft-Windows-TaskScheduler%4Maintenance evtx
Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Admin evtx
Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx
Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Admin evtx
Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx
Logs\Microsoft-Windows-Store%4Operational.evtx
Logs\Microsoft-Windows-UniversalTelemetryClient%4Operational.evtx
Logs\Microsoft-Windows-User Profile Service%4Operational.evtx
Logs\Microsoft-Windows-UserPnp%4ActionCenter.evtx
Logs\Microsoft-Windows-UserPnp%4DeviceInstall evtx
Logs\Microsoft-Windows-VolumeSnapshot-Driver%4Operational.evtx
Logs\Microsoft-Windows-Wcmsvc%4Operational.evtx
Logs\Microsoft-Windows-Windows Defender%4Operational.evtx
Logs\Microsoft-Windows-Windows Defender%4WHC.evtx
Logs\Microsoft-Windows-Windows Firewall With Advanced Security%4ConnectionSecurity evtx
Logs\Microsoft-Windows-WinINet-Config%4ProxyConfigChanged.evtx
Logs\Microsoft-Windows-Winlogon%4Operational evtx
Logs\Microsoft-Windows-WinRM%4Operational.evtx
Logs\Setup evtx
Logs\Windows PowerShell.evtx
Logs\Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall evtx
Logs\Microsoft-Windows-WMI-Activity%4Operational.evtx
Logs\System evtx
Logs\Security.evtx
Windows\System32\winevt\Logs\Setup.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-02-27-12-21-20-622.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-11-20-46-32-189.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-06-30-13-45-03-347.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-08-02-26-04-899.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-10-30-19-26-37-188.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-04-08-05-33-867.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-30-16-29-10-602.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-15-15-07-04-381.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-02-02-52-11-569.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-04-19-00-10-16-214.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-26-22-08-42-827.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-11-22-05-26-089.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-23-04-20-21-835.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-05-26-12-11-25-223.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-04-15-07-09-24-325.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-04-04-35-23-707.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-04-07-21-05-41-859.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-18-19-18-33-633.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-09-23-20-20-681.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-07-22-53-09-400.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-19-09-05-03-069.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-19-03-17-30-918.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-10-02-11-09-22-083.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-09-15-51-43-896.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-09-19-15-04-259.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-28-04-14-58-545.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-06-04-10-43-774.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-24-00-59-56-063.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-08-17-03-22-249.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-10-09-23-03-203.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-06-16-37-56-482.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-02-15-06-36-405.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-07-05-51-17-641.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-03-06-06-07-29-506.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-10-27-06-12-01-889.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-14-02-20-35-061.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-03-16-20-09-20-723.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-26-09-07-58-407.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-07-08-10-16-08-709.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-26-06-16-16-735.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-21-16-36-38-559.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-03-08-53-17-828.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-10-23-15-37-23-347.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-13-00-00-07-540.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-21-03-24-37-573.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-01-15-03-21-17-842.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-10-01-06-03-529.evtx
```

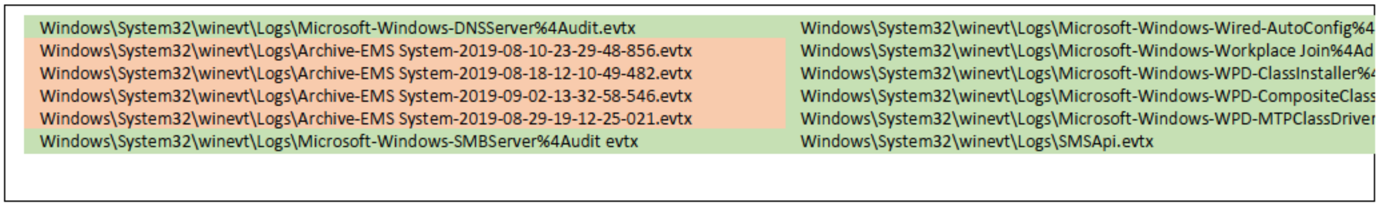
```
Windows\System32\winevt\Logs\Microsoft-Windows-User Profile Servi
Windows\System32\winevt\Logs\Microsoft-Windows-LiveId%4Operatio
Windows\System32\winevt\Logs\Microsoft-Windows-SMBClient%4Ope
Windows\System32\winevt\Logs\Microsoft-Windows-SmbClient%4Con
Windows\System32\winevt\Logs\Microsoft-Windows-SmbClient%4Secu
Windows\System32\winevt\Logs\Microsoft-Windows-Winlogon%4Ope
Windows\System32\winevt\Logs\Microsoft-Windows-SettingSync%4Op
Windows\System32\winevt\Logs\Microsoft-Windows-SettingSync%4De
Windows\System32\winevt\Logs\Microsoft-Windows-DateTimeControl
Windows\System32\winevt\Logs\Microsoft-Windows-Known Folders A
Windows\System32\winevt\Logs\Microsoft-Windows-Shell-Core%4Acti
Windows\System32\winevt\Logs\Microsoft-Windows-Shell-Core%4Ope
Windows\System32\winevt\Logs\Microsoft-Windows-Shell-Core%4App
Windows\System32\winevt\Logs\Microsoft-Windows-Shell-Core%4Logo
Windows\System32\winevt\Logs\Microsoft-Windows-AppXDeployment
Windows\System32\winevt\Logs\Microsoft-Windows-AppModel-Runti
Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-D
Windows\System32\winevt\Logs\Microsoft-Windows-Store%4Operatio
Windows\System32\winevt\Logs\Microsoft-Windows-PushNotification-
Windows\System32\winevt\Logs\Microsoft-Windows-PushNotification-
Windows\System32\winevt\Logs\Microsoft-Windows-TWinUI%4Operat
Windows\System32\winevt\Logs\Microsoft-Windows-Application-Expe
Windows\System32\winevt\Logs\Microsoft-Windows-Application-Expe
Windows\System32\winevt\Logs\Microsoft-Windows-Application-Expe
Windows\System32\winevt\Logs\Microsoft-Windows-Application-Expe
Windows\System32\winevt\Logs\Microsoft-Windows-Security-SPP-UX-
Windows\System32\winevt\Logs\Microsoft-Windows-BackgroundTaskI
Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-M
Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-M
Windows\System32\winevt\Logs\Microsoft-Windows-Forwarding%4Op
Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-M
Windows\System32\winevt\Logs\Microsoft-Windows-Resource-Exhaus
Windows\System32\winevt\Logs\Microsoft-Windows-DataIntegrityScan
Windows\System32\winevt\Logs\Microsoft-Windows-DataIntegrityScan
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Schedu
Windows\System32\winevt\Logs\Microsoft-Windows-HomeGroup Cont
Windows\System32\winevt\Logs\Microsoft-Windows-Shell-ConnectedA
Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-M
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-DPS%4
Windows\System32\winevt\Logs\Microsoft-Windows-Storage-ClassPnP
Windows\System32\winevt\Logs\Microsoft-Windows-RestartManager%
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-PLA%4
Windows\System32\winevt\Logs\Microsoft-Windows-CAPI2%4Operatio
Windows\System32\winevt\Logs\Microsoft-Windows-WindowsUpdateC
Windows\System32\winevt\Logs\Microsoft-Windows-NlaSvc%4Operati
Windows\System32\winevt\Logs\Microsoft-Windows-PowerShell%4Op
Windows\System32\winevt\Logs\Microsoft-Windows-PowerShell%4Ad
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-PCW%4
Windows\System32\winevt\Logs\Microsoft-Windows-Storage-Storport%
Windows\System32\winevt\Logs\EMS System.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Application Serve
Windows\System32\winevt\Logs\Microsoft-Windows-Application Serve
Windows\System32\winevt\Logs\DVS Adjudication.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-CloudStorageWiz
Windows\System32\winevt\Logs\Microsoft-AppV-Client%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-AppV-Client%4Operational
Windows\System32\winevt\Logs\Microsoft-AppV-Client%4Virtual Appli
Windows\System32\winevt\Logs\Microsoft-Rdms-UI%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Rdms-UI%4Operational.evt
Windows\System32\winevt\Logs\Microsoft-User Experience Virtualizati
Windows\System32\winevt\Logs\Microsoft-User Experience Virtualizati
Windows\System32\winevt\Logs\Microsoft-User Experience Virtualizati
Windows\System32\winevt\Logs\Microsoft-User Experience Virtualizati
Windows\System32\winevt\Logs\Microsoft-Windows-AAD%4Operation
Windows\System32\winevt\Logs\Microsoft-Windows-All-User-Install-A
Windows\System32\winevt\Logs\Microsoft-Windows-AllJoyn%4Operat
Windows\System32\winevt\Logs\Microsoft-Windows-AppHost%4Admi
Windows\System32\winevt\Logs\Microsoft-Windows-AppID%4Operati
Windows\System32\winevt\Logs\Microsoft-Windows-ApplicabilityEngin
Windows\System32\winevt\Logs\Microsoft-Windows-AppLocker%4EXE
Windows\System32\winevt\Logs\Microsoft-Windows-AppLocker%4MS
Windows\System32\winevt\Logs\Microsoft-Windows-AppLocker%4Pac
Windows\System32\winevt\Logs\Microsoft-Windows-AppLocker%4Pac
Windows\System32\winevt\Logs\Microsoft-Windows-AppxPackaging%4
Windows\System32\winevt\Logs\Microsoft-Windows-AssignedAccess%
Windows\System32\winevt\Logs\Microsoft-Windows-AssignedAccessB
Windows\System32\winevt\Logs\Microsoft-Windows-Audio%4Capture
```



Windows\System32\winevt\Logs\Archive-EMS System-2019-11-25-05-09-12-916.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Audio%4Operati
Windows\System32\winevt\Logs\Archive-EMS System-2021-01-22-13-12-21-043.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Audio%4Playbac
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-06-08-06-21-993.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Authentication U
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-05-17-16-37-197.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Backup.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-16-23-08-11-827.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-BestPractices%4
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-17-01-19-18-484.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Biometrics%4Op
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-21-01-39-07-647.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Bits-Client%4Ope
Windows\System32\winevt\Logs\Archive-EMS System-2021-03-04-12-10-17-214.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Bluetooth-BthLE
Windows\System32\winevt\Logs\Archive-EMS System-2020-07-12-02-56-47-489.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Bluetooth-MTPE
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-21-07-26-54-297.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-BranchCacheSM
Windows\System32\winevt\Logs\Archive-EMS System-2020-04-04-04-03-42-737.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-CertificateService
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-16-16-31-58-059.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-CertificateService
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-21-12-09-41-781.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-CertificateService
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-28-14-04-05-771.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Compat-Appraise
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-12-22-02-14-487.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-CoreApplication
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-13-18-05-49-770.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-CorruptedFileRec
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-17-19-10-01-322.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-CorruptedFileRec
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-05-14-13-33-324.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DAL-Provider%4
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-14-13-10-56-695.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DeviceGuard%4
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-28-22-08-50-835.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Devices-Backgrou
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-17-11-04-36-787.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DeviceSync%4Op
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-05-00-03-39-390.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Scripte
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-12-10-03-10-333.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Scripte
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-19-20-40-41-039.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Scripte
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-24-11-15-42-872.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-Netw
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-18-17-48-53-388.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DirectoryService
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-09-10-14-15-715.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DiskDiagnostic%4
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-31-11-01-47-908.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DiskDiagnosticDa
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-27-08-29-08-399.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DiskDiagnosticRe
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-14-23-29-04-158.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DSC%4Admin.evt
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-24-21-04-12-832.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DSC%4Operation
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-21-04-04-25-803.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EapHost%4Oper
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-01-07-03-50-651.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EapMethods-Ras
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-14-18-29-08-151.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EapMethods-Ras
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-11-21-02-29-740.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EapMethods-Sim
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-03-11-33-19-283.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EapMethods-Ttls
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-19-20-02-44-037.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EDP-Audit-Regul
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-28-20-58-32-283.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EDP-Audit-TCB%4
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-16-03-02-57-774.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EmbeddedAppLa
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-01-21-14-15-340.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EnrollmentPolicy
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-13-08-12-31-149.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EnrollmentWebS
Windows\System32\winevt\Logs\Archive-EMS System-2020-04-22-17-12-11-701.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EventCollector%4
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-16-05-45-04-636.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Fault-Tolerant-H
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-05-12-32-06-091.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-FederationServic
Windows\System32\winevt\Logs\Archive-EMS System-2021-03-26-13-42-04-162.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-FileServices-Serv
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-16-14-59-42-045.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-FileServices-Serv
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-23-13-23-46-471.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-FileShareShadow
Windows\System32\winevt\Logs\Archive-EMS System-2020-05-18-23-53-08-392.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-FMS%4Operatio
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-21-13-14-26-512.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Folder Redirectio
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-27-17-59-53-690.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-NdisImPlatform%
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-20-09-29-41-350.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-GenericRoaming
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-20-07-59-19-878.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Help%4Operatio
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-31-02-47-11-038.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Hyper-V-Guest-D
Windows\System32\winevt\Logs\Archive-EMS System-2021-01-29-23-11-26-924.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-IdCtrls%4Operati
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-09-05-29-49-411.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-IKE%4Operationa
Windows\System32\winevt\Logs\Archive-EMS System-2021-01-26-06-11-56-096.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-International-Reg
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-23-00-00-39-858.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-KdsSvc%4Operat
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-14-18-58-50-004.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-ApphelpC
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-28-08-06-44-934.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-EventTrac
Windows\System32\winevt\Logs\Archive-EMS System-2020-04-11-14-07-34-718.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-WDI%4Op
Windows\System32\winevt\Logs\Archive-EMS System-2020-05-15-07-27-29-016.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-LanguagePackSet
Windows\System32\winevt\Logs\Archive-EMS System-2020-07-04-17-16-43-223.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-ManagementTo
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-24-22-45-04-435.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-ManagementTo
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-20-18-16-33-823.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-MemoryDiagnost
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-18-12-49-02-987.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-MiStreamProvide
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-13-08-24-43-079.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Mobile-Broadba
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-22-12-08-49-154.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Mobile-Broadba
Windows\System32\winevt\Logs\Archive-EMS System-2021-03-30-02-15-24-619.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Mprddm%4Oper
Windows\System32\winevt\Logs\Archive-EMS System-2020-05-22-17-53-50-782.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-MsLbfoProvider%
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-11-17-12-21-460.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-NetworkLocatio
Windows\System32\winevt\Logs\Archive-EMS System-2021-01-18-20-12-44-811.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-NetworkProvider
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-02-14-34-04-967.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-NTLM%4Operati
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-07-10-51-04-386.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-OfflineFiles%4Op
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-11-05-09-09-286.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-OneBackup%4De
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-31-12-27-41-741.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-OOBE-Machine-
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-22-20-55-04-936.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-PackageStateRoa



Windows\System32\winevt\Logs\Archive-EMS System-2020-07-01-03-27-07-105 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Partition%4Diagr
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-09-17-04-07-509 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-PerceptionRuntir
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-09-07-12-48-391 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-PerceptionSenso
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-11-00-11-12-292 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-User Control Pan
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-15-12-21-57-907 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Policy%4Operatic
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-03-08-03-17-087 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-PowerShell-Desir FileDownloadManager%4Operational evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-22-18-13-07-673 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-PrintBRM%4Adm
Windows\System32\winevt\Logs\Archive-EMS System-2020-08-27-17-53-57-312 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-PrintService%4Ac
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-30-01-16-19-620 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-ReadyBoost%4Op
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-20-19-51-20-073 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-ReFS%4Operatio
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-13-02-24-44-262 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Regsvr32%4Oper
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-15-23-57-17-682 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-RemoteApp and
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-08-20-31-15-022 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-RemoteApp and
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-09-21-34-01-652 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-RemoteDesktopS
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-02-16-11-00-907 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-RemoteDesktopS
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-10-17-14-18-337 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-RemoteDesktopS
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-17-16-31-18-634 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-RemoteDesktopS
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-09-17-35-55-190 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Resource-Exhaus
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-10-17-26-50-697 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-ScmBus%4Certifi
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-08-21-07-21-169 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-ScmDisk0101%4C
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-09-22-01-49-473 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SearchUI%4Oper
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-18-15-41-56-864 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Security-Audit-Cc
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-09-17-14-16-397 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Security-Enterpri
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-09-17-25-20-742 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Security-Netlogo
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-09-17-33-50-215 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Security-SPP-UX-
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-09-17-46-57-607 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Security-UserCon
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-16-17-20-24-507 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-ServerEssentials-
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-14-07-23-24-216 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-C
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-12-14-51-41-139 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SettingSync-Azur
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-18-04-06-37-355 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SettingSync-Azur
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-18-09-54-24-839 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SilProvider%4Op
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-19-14-52-50-172 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SmartCard-Audit
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-22-06-37-33-489 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SmartCard-Devic
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-12-03-16-22-000 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SmartCard-TPM-
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-21-19-02-14-166 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SmartCard-TPM-
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-22-00-50-01-529 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SMBDirect%4Adr
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-14-01-35-37-340 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SMBWitnessClier
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-13-14-00-17-879 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SMBWitnessClier
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-23-17-23-46-597 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Storage-Tiering%
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-12-20-37-42-553 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-StorageManagem
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-12-09-03-54-186 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-D
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-17-10-43-31-360 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-D
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-17-04-55-44-339 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-Sp
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-17-22-18-50-801 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-Sp
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-13-19-47-50-347 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SystemSettingsTh
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-15-06-34-10-708 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TCPIP%4Operatic
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-20-02-28-13-043 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-18-21-29-43-807 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-15-00-46-23-325 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-15-18-09-30-390 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-20-14-03-47-942 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-23-11-36-14-332 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-16-11-32-36-872 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-20-08-16-00-636 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-23-05-48-27-189 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-22-12-25-20-731 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Microsoft-Windows-UniversalTelemetryClient%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Microsoft-Windows-NetworkProfile%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-StoreMgr%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Microsoft-Windows-SMBServer%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TZSync%4Operat
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-19-09-27-36-681 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TZUtil%4Operatic
Windows\System32\winevt\Logs\Microsoft-Windows-SMBServer%4Security.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-UAC%4Operatior
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-23-03-48-10-012 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-UAC-FileVirtualiz
Windows\System32\winevt\Logs\Microsoft-Windows-SMBServer%4Connectivity.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-User Device Regis
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-14-17-50-17-089 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-User-Loader%4O
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-22-06-31-22-632 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-VerifyHardwareS
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-03-10-49-41-423 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Volume%4Diagnc
Windows\System32\winevt\Logs\Microsoft-Windows-Dhcp-Server%4Operational evtx	Windows\System32\winevt\Logs\Microsoft-Windows-VPN-Client%4Op
Windows\System32\winevt\Logs\Microsoft-Windows-Dhcp-Server%4FilterNotifications.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-VPN%4Operation
Windows\System32\winevt\Logs\DhcpAdminEvents.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-WFP%4Operatior
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-26-00-51-55-728 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Win32k%4Opera
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-07-05-09-14-598 evtx	Windows\System32\winevt\Logs\Microsoft-Windows-WindowsSystem
Windows\System32\winevt\Logs\DNS Server.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Winsock-WS2HEL



Windows\System32\winevt\Logs\Microsoft-Windows-DNSServer%4Audit.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Wired-AutoConfig%4
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-10-23-29-48-856.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Workplace Join%4Ad
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-18-12-10-49-482.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-WPD-ClassInstaller%4
Windows\System32\winevt\Logs\Archive-EMS System-2019-09-02-13-32-58-546.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-WPD-CompositeClass
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-29-19-12-25-021.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-WPD-MTPClassDriver
Windows\System32\winevt\Logs\Microsoft-Windows-SMBServer%4Audit evtx	Windows\System32\winevt\Logs\SMSApi.evtx

Analysis Summary

Analysis of the Mesa County Dominion Voting Systems EMS server identified that extensive deletion of both election data and election-related data, comprising election records which must and should have been preserved under Federal and Colorado law, has occurred either as a result of or coincident with the vendor's and CO Secretary of State's modification of the system from version 5.11-CO to 5.13. This deleted data is critical to any effort to reconstruct events taking place on the voting systems, and to determine if unauthorized access or operation of the voting systems took place.

Furthermore, the EMS server application logging functions are configured to "Overwrite events as needed" if arbitrarily-selected file storage sizes are exceeded, which could predictably and likely has resulted in the systematic, automated deletion of logfile content comprising election-related data.

This systemic deletion of logfile data requires additional investigation.

CONCLUSION

This forensic examination found that significant election record preservation requirements under the 2002 VSS and Federal and state law HAVE NOT BEEN MET and further that destruction of Election-Related Data, specifically critical logfiles, has occurred. This destruction is not incidental or minor but is *highly significant*.

These findings have been demonstrated in this report and evidence has been presented demonstrating *conclusively to both computer systems experts as well as legal professionals and the general public at large* that the facts in these findings support the conclusions that:

1) Election-related data and election data explicitly required to be preserved, as described in the 2002 VSS criteria referenced in this section, HAS BEEN DESTROYED IN VIOLATION OF THE LAW, and

2) The specific configuration settings of the server examined lead to the understanding that Certification Requirements for Voting Systems have likely not been met despite this system having been certified and thereby approved for use in Colorado by the Colorado Secretary of State.

Further investigation is required to determine the full scope of non-compliance with legal mandates for voting systems and election records, and whether the non-compliance is deliberate or simply negligent.

Doug Gould Biography

Doug Gould is an expert in Cyber Security with more than 40 years' experience in the field. Doug retired from AT&T after 31 years, where he served as Chief Cyber Security Strategist. He currently serves as Chief Technical Officer at CyberTeamUS.

Doug began at AT&T with Bell Laboratories, serving in the Semiconductor Laser Development department and later in the Bell Lab's Security Group, as a delegate to the Bell Labs' Unix Systems Subcommittee, was an early pioneer in the field of Computer Forensics and won a Bell Labs Innovation Award. At AT&T he designed the security architecture for one of the largest states in the US, consulted with cabinets of the nations' largest corporations and designed the first healthcare network fully compliant with Healthcare Information Exchange standards. Outside AT&T, he has overseen security for a US Government Agency and has solved major cases for the FBI and Secret Service; he has served as an Officer of the Court as a forensic expert and has been an expert witness in landmark cybersecurity cases. He designed security architectures for DoD networks including some of the most sensitive areas of the Government. Doug has owned and led several professional services firms in the Information Security field. He served on the NC Council for Entrepreneurial Development and has consulted with many companies about the complex integration of business and technology.

Doug is the past president of Eastern North Carolina InfraGard, the public-private partnership between the nation's critical infrastructure operators and the US Intelligence community.

Doug's background is at the Master's level in Electrical Engineering, Computer Science, Computer Security and Business Administration.

He is a subject matter expert in:

- Strategic Enterprise Security
- Security Architecture & Design (including network Micro-Segmentation)
- Security Governance
- Risk Management
- Security Device Technologies (Firewalls, IDS/IPS, DLP, SIEMs, Encryption, VPNs, Unified Threat Management, etc., Enterprise, Remote and Cloud)
- Information Forensics (Computer & Network Forensics)
- Public Key Infrastructures
- Identity and Access Management
- Authentication, Authorization and Access Control (incl Biometrics)
- Regulatory Compliance
- Physical Security (Threat Assessment/Risk Analysis, TSCM, Access Control, Counterterrorism & Counterintelligence, facility and site protection)
- Business Continuity & Disaster Recovery Planning
- Response & Recovery Strategy
- Threat Intelligence
- Intelligence Analysis

Doug served as Chief Information Security Officer at the World Institute for Security Enhancement, has written advanced security courses, developed advanced security methodologies and has taught government, private sector professionals and law enforcement agents information security, computer forensics, advanced computer forensic sciences and Technical Surveillance Countermeasures (TSCM).

Doug holds numerous certifications in security including the CISSP and Certified Anti-Terrorism Specialist (CAS), as well as numerous instructor certifications in security.

Doug currently serves as Chief Technical Officer at CyberTeamUS.

He is a Vietnam-era US Navy Veteran where he worked in Electronic Warfare and Electronic Intelligence.

Doug is an invited conference speaker.

EXHIBIT

G

Doug Gould Forensic Addendum

Major Forensic Cases

- 1986 – Disclosure of National Security Information
  Discovered a leak of highly classified information and was able to identify the perpetrator within a group of 15 people. The FBI and US Naval Investigative Service brought this to resolution.
- Early 1990's – US Secret Service investigation, "Mothers of Doom" hacker case
  At USSS Evidence Lab, in response to a request for assistance from USS SA Jack Lewis, performed evidence recovery and identified 800 pages of evidence, invalidating immunity of a suspect's testimony in a proffer session.
- Late 1990's – Interpath, a North Carolina Internet Service Provider (ISP)
  This ISP was a tier-1 (top level) provider infected with Stacheldraht malware. Investigated the live (running) server and identified that all evidence on disc had been deleted. The only remaining evidence was a running program in memory, which was recovered. This case changed the Best Practice in Forensics – no longer is the first step necessarily removing the power. Had that been done no evidence would remain in this case.
- Late 1990's – As senior security administrator for the US EPA, investigated a complaint from the White House of computer intrusions and discovered an international attack involving 4 countries. Wrote monitoring and tracking software to capture the perpetrator online, brought together the FBI, Royal Canadian Mounted Police (RCMP), Scotland Yard and Deutche Bundespost in a live investigation tracking the intruder resulting in an arrest in Germany.
- South Carolina – A Public Works supervisor accused of violation of county policy was fired and brought countersuit. Forensic investigation recovered 4 3" thick binders of evidence showing sexual misconduct. Countersuit dismissed.
- Discovered Al Qaida attack plans targeting US Soil. Working with the FBI, the perpetrator, who was a foreign citizen in the US. Arrest made within 48 hours and the attack was thwarted.
- Mid-2000's – Florida vs. Rabinowicz – in a case where possession of contraband was the only element of proof, stipulated that the contraband was authentic and present. I proved forensically that the defendant was not technically in possession of the evidence and that evidence was planted. Qualified as an expert witness and provided expert testimony in this case.
- Mid-2000's – Identified a leak of national security from Oak Ridge National Laboratory involving chemical weapon information using forensic analysis and was able to identify the perpetrator. DSS responded and resolved the case.
- Mid-2000's – Investigated sabotage of a health industry contractor. The systems administrator had been fired and sabotaged the system. Solved the case and the administrator went to prison.

Instructor of Forensics

- Taught Forensics and Advance Forensic Techniques to State Law Enforcement, Military and major corporate customers at the World Institute for Security Enhancement.
- Taught Technical Surveillance Countermeasures (TSCM) course for government and industry at the World Institute for Security Enhancement.
- Wrote the entire course and taught the entire CISSP curriculum at Able Information Systems.